2015-1

Context-Based Access for Infrequent Requests in Tanzania's Health Care System

Zanifa Omary
Technological University Dublin, zanifa.omary@student.dit.ie

Context-Based Access for Infrequent Requests in Tanzania's Health Care System

Thesis Submitted

By

Zanifa Omary

Supervisors:

Dr. Fredrick J. Mtenzi

Prof. Bing Wu

School of Computing

Dublin Institute of Technology

Kevin Street, Dublin 8, Dublin, Ireland

To the Office of Postgraduate Studies and Research at the Dublin Institute of Technology in the fulfilment of the requirements for the Degree of Doctor of Philosophy

Jan. 2015

In the loving memory of my late father, ***Omary J.P.L. (Jan. 1952 - Mar. 2012)*** *and my nephew* ***Nasir M.K. (22 May 2011 - 21 Feb 2013)***

Dear Father, it is with great sadness that you are no longer with us and you can't read this, I am writing to let the "world" know I finished this Doctorate for you and I miss you dearly.

Nasir, you will always live in my heart.

Abstract

Access control is an important aspect of any information system. It is a way of ensuring that users can only access what they are authorised to and no more. This can be achieved by granting users access to resources based on pre-defined organisational and legislative rules. Although access control has been extensively studied, and as a result, a wide range of access control models, mechanisms and systems have been proposed, specific access control requirements for healthcare systems that needs to support the continuity of care in an accountable manner have not been addressed. This results in a gap between what is required by the application domain and what is actually practised, and thus access control solutions implemented for the domain become too restrictive. The continuity of care is defined as the delivery of seamless health care services to patients through integration, coordination and sharing of information between providers. This thesis, therefore, designs a context-based access control model that allows healthcare professionals to bypass access rules in an accountable manner in case of an infrequent access request involving an emergency situation. This research uses the Tanzania's healthcare system as a case study domain.

The contributions from this thesis to the body of knowledge are as follows:

1. A generic methodological approach, named COIL, for gathering comprehensive access control requirements in the healthcare domain is developed. The proposed COIL methodology is the synthesis of four elements: contexts, privacy and security capabilities from national electronic healthcare initiatives, legislations and organisational rules. Each of the four components of the COIL approach has its own impact in relation to access to electronic health records.

2. A taxonomy for classifying access control models is also proposed in this thesis. The intent of the proposed taxonomy is to identify how existing access control models can be classified classified against the proposed Role and Context-Based

Access Control (RoC-BAC) model.

3. To support the continuity of care in an accountable manner, a new context-based access control model is proposed. The Role and Context-Based Access Control model is developed for the healthcare domain, and it is an extension of traditional Role-Based Access Control (RBAC) model with health-related contexts and obligations.

4. With the proposed RoC-BAC model, a new concept of health-related contexts is also introduced. It represents specific contexts from the healthcare domain that should be evaluated by an access control system in order to support the continuity of care.

5. A prototype that implements Role and Context-Based Access Control model is developed. The prototype, called CEATH (Context-Enhanced Access in a Tanzania Healthcare) system, was developed so as to achieve two purposes: 1. to demonstrate that RoC-BAC model is practical and, 2. to evaluate the performance overheads introduced by new entities and relations. Through its support of context-based policies, and especially health-related contexts, it has been demonstrated in this thesis that the incorporation of health-related contexts and obligations helps healthcare professionals to bypass access rules in an accountable manner in case of unexpected emergency situation, which in turn supports the continuity of care.

Declaration

I certify that this thesis which I now submit for examination for the award of Doctor of Philosophy, is entirely my own work and has not been taken from the work of others, save and to the extent that such work has been cited and acknowledged within the text of my work.

This thesis was prepared according to the regulations for postgraduate study by research of the Dublin Institute of Technology, hereafter referred to as the Institute, and has not been submitted in whole or in part for another award in any Institute.

The work reported on in this thesis conforms to the principles and requirements of the Institute's guidelines for ethics in research.

The Institute has permission to keep, lend or copy this thesis in whole or in part, on condition that any such use of the material of the thesis be duly acknowledged.

. . . . . .

Zanifa Omary

Jan. 2015

Acknowledgements

I would like to express my sincere gratitude and appreciation to special people who very much deserve my special thanks for their generous help and support during my graduate career.

First and foremost I am grateful to my supervisors, Dr. Fredrick Japhet Mtenzi and Prof. Bing Wu, from the School of Computing at the Dublin Institute of Technology (DIT). I am extraordinarily grateful to my primary supervisor, Dr. Mtenzi, who was always available whenever I needed his help.

Special appreciation and thanks also goes to my second supervisor Prof. Bing Wu. Despite his tight schedule he always had time for me. His warm words of encouragement during my studies were essential. Thank you.

I am also grateful to past and present staff from the School of Computing whom I have worked with including Prof. Brendan O'Shea, Dr. Deidre Lillis, Ms. Denise Murray, Dr. Ronan Fitzpatrick and Mr. David Ng. My appreciation also goes out to Raffaella Salvante, Gerolmina Di Nado and Conor McCague from the Graduate school for their constant help when the need arises.

To my surviving parent, thank you very much for your love, endless support and encouragement that you have shown throughout these years. To my lovely sisters, brothers, aunties, uncles and all the extended family members, thank you very much for all the advice and encouragement. I

can not remember how many times a simple talk with you guys turned my life into a fresh start.

Finally to all my friends, A very special thank you for your practical and emotional support. I feel blessed to have each and every single one of you in my life.

Contents

List of Tables

List of Figures

Nomenclature & Abbreviations

ABAC	Attribute-Based Access Control
ACL	Access Control List
ACM	Access Control Matrix
AT	Authorisation Table
BTG	Break-The-Glass
CEATH	Context- Enhanced Access in a Tanzania Healthcare system
CL	Capability List
COIL	Contexts, Organisational rules, e-health Initiatives and Legislative rules
DAC	Discretionary Access Control
DH	Department of Health
EHR	Electronic Health Record
HIPAA	Health Insurance Portability and accountability Act
ICT	Information and Communication Technologies
MAC	Mandatory Access Control
MCDGC	Ministry of Community Development, Gender and Children

MoHSW	Ministry of Health and Social Welfare
NCRS	National Care Record Service
NDAC	Non-Discretionary Access Control
NEHR	National Electronic Health Record
NEHTA	National E-Health Transition Authority
NHS	National Health Service
NIST	National Institute of Standards and Technology
NPfIT	National Programme for Information Technology
PHSDP	Primary Health Services Development Programme
TCSEC	Trusted Computer Security Evaluation Criteria
WHO	World Health Organisation
XACML	eXtensible Access Control Markup Language

Chapter 1

Introduction

This chapter is organised as follows: Section 1.1 opens this thesis with a discussion on researcher's motivations behind a research in electronic healthcare. Section 1.2 analyses one of the major challenges in electronic healthcare, that is security, by discussing factors that contribute to breaches in electronic healthcare information systems. Section 1.3 presents the main focus of this thesis in terms of research problem, implementation approach and research aim and objectives. The research methodology adopted in this thesis is discussed in Section 1.4, followed by expected contributions to the body of knowledge in Section 1.5. The list of publications associated with this research work are listed in Section 1.6. An outline of the thesis is provided in Section 1.7.

1.1 Research Motivation

The ever increasing use of information and communication technologies affects almost every aspect of our lives from business, government to entertainment. In business, the usage of Information and Communication Technologies (ICTs) has significantly improved customer services, lowered costs and standardised processes and operations. ICT has also been used in public services by the governments to enable citizens, enterprises and organisations to easily, quickly and at a lower cost to conduct businesses with the government. Despite its successful adoption and use in other domains, the usage of ICT in healthcare is still very low. It has been noted by researchers from academia and industry that, the usage of ICT in healthcare as compared to other industries is behind by as much as ten to fifteen years (Goldschmidt, 2005).

Although many healthcare professionals around the world recognise the benefits introduced by ICT, they also cite various barriers hindering their implementations in practice. Among their reasons include lack of access to capital, complexity of electronic healthcare information systems, lack of standards to permit exchange of clinical data, and unavailability of reliable evidence to suggest economic impact of using ICT to deliver high quality care. The latter reason is a result of overestimation of its results and unfounded expectations (Tan, 2005), (Shekelle *et al.*, 2006), (Stroetmann *et al.*, 2006), (Anderson, 2007). The healthcare domain also faces resistance from healthcare professionals to acquire and commit to new mindset and skills, and resistance to adapt and learn new skills and competencies. In some countries, like Tanzania, the healthcare domain also suffers from the lack of national policies and regulatory frameworks that are designed to reduce the impact of external factors in ICT adoption. In addition to these challenges, healthcare as a domain suffers from issues that go beyond medical problems that could benefit from the adoption and use of ICT. Some of these problems include lack of highly qualified healthcare personnel, rapidly

ageing population, increase in the number of non-communicable and life style diseases and also an increase in the number of people living with some form of disability.

In case of a rapid ageing population, the World Health Organisation (WHO) reports that the proportion of people aged sixty-five years and older is growing faster than any other age group in human history (World Health Organisation, 2012a). On their 2012 report on world population ageing, the United Nations, for instance, estimated that the number of people aged sixty-five years and older will double as a proportion of the global population, from 7% in 2000 to 16% in 2050 (United Nations DESA, 2012). Both longer life expectancy (44 years in 1950, estimated to be 77 years in 2050) and an alarmingly declining fertility rates are considered as the main contributors for such a rapid ageing population (World Health Organisation, 2012a). In relation to healthcare and the need for human resources for health, the aged population is likely to suffer from age-related diseases such as cardiovascular diseases, diabetes and Alzheimer and require long-term care.

Similarly, there is a rise in a number of non-communicable and lifestyle diseases which are chronic and expensive to treat. On its global status report on non-communicable diseases, the WHO noted that out of fifty seven million deaths that occurred globally in the year 2008, thirty six million were due to non-communicable and life style diseases (World Health Organisation, 2011). To highlight more on this, in a report published by the World Health Organisation (2005), China is estimated to lose about US $558 billion in national income between 2006 and 2015 from deaths due to a combination of heart diseases, stroke and diabetes. The increase in chronic health conditions and the rise in world's ageing population go hand in hand with disability. As of September 2013, it was estimated that more than one billion people, which is about 15% of the world population were living with some form of disability (World Health Organisation, 2012b). It is common especially in developing countries for people with disabilities

(about 8%) to have less access to healthcare services hence experience unmet healthcare needs (World Health Organisation, 2013b).

Since Electronic Health Record (EHR) resides at the centre of any electronic healthcare information system, its adoption and use results in numerous benefits to patients, healthcare professionals, healthcare organisation and the government as a whole. In this thesis, EHR represents a lifetime record of a patient with key health history and care within the healthcare system. They enable faster, safer and better healthcare services to patients by providing access to medical information "to the right hands in the right time". The EHRs also improve patient safety as they provide an overview of clinical and medical history, which in turn helps to avoid potential errors and complications (Eysenbach, 2001), (Grimson, 2001), (Wyatt & Sullivan, 2005), (Paulson & Snyder, 2005), (Tan, 2005), (Shekelle *et al.*, 2006), (Mukherjee & McGinnis, 2007). Furthermore, the adoption of ICT in healthcare also promises better access to specialist care in all geographical areas.

1.2 Access to Medical Records

Regardless of its promise to offer benefits to individuals, healthcare organisations and third party payers to healthcare services (like insurance companies), we read about inappropriate access to medical records on a regular basis. The United States of America is one of the countries where security breaches involving EHRs have been extensively reported (DHHR, 2013). Between 2009 and 2012, about twenty one million patients have had their medical records exposed in data security breaches in the United States of America alone. The reasons leading to their exposure include theft of medical records, which is the most common reason with about fifty four percent (54%) of the overall breaches, lost records and devices with about eleven percent (11%) and hacking with 6%. Although theft and hacking are regarded as the biggest threats to medical

records, it is unauthorised access or disclosure that has been consistently ranked as one of the leading issues. It is second to theft with 20%.

Although there is low reporting on data security breaches in Tanzania and Africa in general due to majority of the implementations being in the infancy stages, several researchers have conducted studies to identify issues, challenges and opportunities of Electronic Health Records from the healthcare consumers' (which are referred as patients throughout this thesis) standpoint. From a survey conducted by Nehemiah (2014) in three hospitals in Tanzania involving 240 participants, the healthcare consumers indicated hacking (79.5%), malicious software (69%), and unauthorised access (70%) as the common problems that could affect EHRs.

Based on the data from America and Tanzania consecutively, it can be noted that, not only will unauthorised disclosure of medical records threaten patients' privacy, it may also inflict significant damage to both patients' health and lives if necessary preventive measures are not established. While patients' lives may be affected due to malicious modification of diagnosis data, their health may be affected by improper use of medical records. The compromise may also result in social embarrassment or prejudice, identity theft, blackmailing and may even affect their insurability. For the healthcare organisation where the compromised medical records are collected, processed, and stored, any security breach may result in monetary loss and damage in reputation.

There are more reasons contributing to data security breaches in electronic healthcare information systems, including:

Digitisation of Records: One of the key benefits that motivates the adoption and use of ICT in healthcare is the digitisation of medical records forming Electronic Health Records (EHRs). Contrary to paper-based records, digitised medical records

allow electronic healthcare information systems to gather and exchange accurate and appropriate data, and thus satisfy clinical, administrative and transactional needs of the healthcare providers, payers as well as other users. These records contain personal identifiable information such as name, date of birth, address, phone number, bank name, routing number and saving and checking number. They also contain a patient's medical history as well as financial and insurance information.

Basically, EHRs contain personal and sensitive clinical information that would allow thieves, for example, to fraudulently open up new lines of credit in their victim's name, if compromised and which will in turn destroy their credit record when they get billed for medical procedures that they didn't even know about. Additionally, EHRs guarantee higher financial pay-outs to the computer hackers. On the black market in the United States of America, for instance, a portion of a single set of patient's EHR can fetch up to $50 compared to $1.50 for credit card information, $3 for date of birth, $3 for social security numbers and $6 for mother's maiden name (Hayes, 2014). The EHRs can fetch larger sum of money because of the availability of more personally identifiable information, in which criminals can use for a whole range of fraudulent activities, including blackmailing (Hayes, 2014). The average payout for a medical identity theft is around $20,000 compared to $2,000 for a regular identity theft (EMC, 2013).

It is also common for stolen EHRs to be used to make false or inflated insurance claims, to obtain addictive prescription drugs or to receive medical treatment at the account holder's expense. To make matters worse for the domain which could highly benefit from adoption and use of ICTs, it takes twice as long to identify medical information fraud compared to regular identity theft. Usually when a bank account is compromised, a victim may delete or change personal information. In healthcare, however, patients' health information cannot be cancelled or altered and neither the

victim nor the healthcare organisation can prevent criminals from using the data. It is also hard to notice when a patient's healthcare information has been compromised, unless there is money involved.

Insecure Code: A successful Electronic Health Record (EHR) is characterised with an ability to follow an individual patient whenever, wherever he or she receives care. This means that medical records of the patient need to be highly shareable between collaborating healthcare providers and systems. To achieve high shareability in the healthcare domain, the electronic healthcare information systems are built using complex software that includes many diverse components, interconnected in multiple ways. As software becomes complex, the ability of a human being to design, develop, produce, distribute, and maintain the software is increasingly challenged (Paul, 2007), (Rice, 2007). Thus, it becomes easy to introduce security flaws (Baskerville, 1993), (Soffa, 2007).

System Integration: In a modern healthcare environment, a Hospital Information System (HIS) can be defined as a computerised system that is designed to meet all information needs within a hospital. It is a full integrated, comprehensive solution that provides healthcare organisations with a wide range of tools for hospital management, clinical tasks and patient administration. HIS may include Clinical Information System, Patient Administration System, Radiology Information System or Picture Archiving and Communication System (PACS), Pharmacy Information Management System (PIS) and Laboratory Information Systems (LIS). Usually, each of these systems is vulnerable to security threats, and integrating them expands the attack surface and therefore increases the chances for a security breach to occur.

1.3 Research Problem

The high growth rate of Internet and mobile phones utilisation in Tanzania in the past decade is a result of a construction of the national fibre optic cable network, known as National ICT Broadband Backbone (NICTBB), and an extensive use of mobile broadband. The implementation of these technologies have had an impact on almost every aspect of an urbanised citizen's life, ranging from business to entertainment. In business, the usage of ICT has significantly improved customer services, lowered costs and standardised processes and operations; in public services, its usage has enabled citizens, enterprises and organisations to easily, quickly and at the lower cost to conduct businesses with the government. Based on availability of ICT, there are various ministries and agencies, including Tanzania Revenue Authority (TRA), which are providing services and conducting business with the citizens efficiently and effectively (Oreku *et al.*, 2011).

In spite of the proliferation of ICT use in numerous application domains in Tanzania, its usage in healthcare is still low. In this thesis, five main reasons have been identified as the contributing factors to this situation. These include

- Lack of training and exposure of healthcare professionals,
- Lack of access to capital by healthcare providers (whether as an individual healthcare provider or a healthcare organisation as a whole),
- Lack of standards to permit the exchange of clinical data
- Lack of legislation and regulations to guide implementations of EHR systems as well as to guide EHRs access and use
- Healthcare professionals' resistance towards adoption and use of information systems and information management systems

As a result of these challenges, Tanzania healthcare system is characterised as a combination of both manual and electronic healthcare system that does not support infrequent access requests in case of emergencies. To better handle infrequent access requests that affect the delivery of seamless health care services to patients through integration, coordination, and sharing of information between providers in a Tanzania healthcare system, this thesis develops a generic methodological approach for gathering comprehensive access control requirements in a healthcare domain and then proposes a new context-based access control model named Role and Context-Based Access Control (RoC-BAC) by extending the traditional Role-Based Access Control (RBAC) model with Break-The-Glass (BTG), using contexts and obligations.

This thesis is designed to address the following research question:

How will the contexts be defined and used to better handle infrequent access requests associated with emergencies in an accountable manner?

This main research question can be narrowed into the following questions that accommodate Tanzania healthcare system, which is used as a case study domain:

1. What are the technical and non-technical challenges facing the Tanzania healthcare system?
2. What are the limitations of the existing approaches designed to control access to electronic health records, and how to utilise them to support the continuity of care?
3. Which access control requirements are addressed into the current electronic healthcare information systems and how were those requirements specified?
4. How can contexts that is specific to the healthcare domain be defined and incorporated into an existing access control solution?

5. Which factors affect the performance of a system that implements Role and Context-Based Access Control (RoC-BAC) against a system that implements traditional Role-Based Access Control (RBAC) model?

1.3.1 Proposed Approach

To address the main research question presented in Section 1.3, a research approach adopted in this thesis involves a specification of access control requirements that are appropriate for healthcare organisations in a Tanzania healthcare system (using the newly designed COIL methodology), developing a new context-based access control model named RoC-BAC that handles better infrequent access requests. In this thesis the proposed COIL methodology is a combination of contexts, privacy and security policies from national e-health initiatives and legislative and organisational rules.

To support the continuity of care by providing flexible access to medical records in an accountable manner, the new RoC-BAC model is an extension of the traditional Role-Based Access Control (RBAC) model with Break-The-Glass using contexts and obligations. With the proposed model, a new concept named health-related contexts is also introduced.

1.3.2 Research Aim and Objectives

The main aim of this research is to design a new context-based access control model that supports the continuity of care by better handling infrequent access requests in an accountable manner. To this end, the following objectives were set:

- To investigate the characteristics of the Tanzania healthcare system, with special consideration on human resources for health and its status on the implementation of electronic healthcare information systems

- To identify which access control requirements are addressed in EHR systems and categorise them, and also to investigate how those access control requirements were obtained
- To evaluate existing access control models and analyse their suitability for the modern healthcare environments
- To examine how contexts are defined and used in various application domains, and how can they be incorporated into an access decision of an electronic healthcare system
- To propose a new context-based access control model that addresses infrequent access requests into its access decision
- To implement a prototype for both role based access control and a new context-based access control in order to evaluate performance overheads introduced by contexts and obligations into the Role and Context-Based Access Control (RoC-BAC) model.

1.4 Methodology

The research methodology adopted for this thesis involves a combination of desk research, data collection and prototyping. Mainly, it consists of a literature review, data collection, designing and formalisation of a context-based access control model, and prototype design and development as well as evaluation. Each component of the research methodology are discussed herein

1. **Literature Review:** To gain a comprehensive understanding of the challenges addressed by this study, a literature survey in relation to the Tanzania's healthcare system and access control models and mechanisms was conducted. This analysis

led to the general understanding of the Tanzania's healthcare system, discussed in Chapter 2 and also a thorough understanding of the limitations of the existing access control models for the healthcare domain, discussed in Chapter 3. Moreover, an investigation on traditional access control models offered the basis for further analysis of access control requirements for the healthcare domain as well as theoretical formalisation of the new context-based access control model.

2. **Data Collection:** In this research, data collection was conducted in two phases. While the second phase involved collection of access scenarios from the Tanzania's healthcare system, the first phase involved obtaining real healthcare data for evaluation purposes.

   During the initial stages of this research, and when the overall goal was to design a framework for securing patients' healthcare information, the general procedure for research clearance that would allow the researcher to access real healthcare data in a Tanzania's healthcare system was followed. Three separate permissions were to be obtained before the researcher could be allowed to access healthcare data. The permissions were from: 1. the Ministry of Health and Social Welfare (MoHSW); 2. the National Institute of Medical Research (NIMR) which oversees all the research in the healthcare domain in Tanzania and 3. the hospital that will provide data, in this case the Muhimbili National Hospital (MNH) and Ilala Municipal Council (overseeing the Mnazi Mmoja Health Centre, Amana Hospital and Buguruni Health Centre). In all the six institutions, a research proposal has to be written and submitted. The research proposal is then assessed by Ethical Committee of each institute in terms of the value of its contributions to the general community, feasibility of the research process, and the capability of the researcher to undertake the proposed research.

   The researcher followed the above procedures and the permissions were then granted

by the three main institutions (that is, MoHSW, NIMR and Ilala Municipal Council). The research clearance certificates from NIMR and Ilala Municipal Council are in Appendix A. With these clearance certificates at hand, the DIT Research and Ethics Committee also granted the researcher the DIT Ethical Approval under the condition that no real healthcare data should be used. Based on this restriction and the restrictions of the trans-border data flow in relation to healthcare data, it was agreed with the supervisors that only simulated healthcare data should be used for evaluation. The schema of the dataset used is based on the schema similar to that of the Muhimbili National Hospital (MNH).

The access rules used during evaluation stage in this research were collected from different healthcare facilities in Tanzania. These access rules were obtained partly from an observation survey carried out at the Muhimbili National Hospital (MNH) and a questionnaire distributed to healthcare professionals and systems administrators working in several healthcare facilities within a Tanzania healthcare system. The questionnaire used to obtain the access rules is in Appendix B.

3. **Access Control Requirements:** Since the current healthcare system in Tanzania works with both paper-based and electronic medical records, the first step towards designing a relevant access control model for the domain was to identify adequate access control requirements that would support the continuity of care by better handling infrequent access requests. To help with identification of access control requirements, a new methodology for gathering access control requirements was developed. The newly proposed COIL (Contexts, Organisational rules, e-health Initiatives and Legislative rules) methodology is a result of the synthesization of contexts, privacy and security capabilities from national e-health initiatives, legislative and organisational rules. It allows easy specification of access control requirements and can also be used as a guideline to evaluate access control sys-

tems in a modern healthcare environments. The COIL methodology is discussed in detail in Chapter 4.

4. **Model Design and Formalisation:** This thesis proposes a new context-based access control model named Role and Context-Based Access Control (RoC-BAC) that supports the continuity of care by better handling infrequent access requests. The proposed context-based access control model is the main contribution of this research to the body of knowledge. Its design is divided into two parts: initial high-level design, where a theoretical model was designed during early stages of this research, and a detailed design. With the latter, a detailed model was designed by extending the traditional Role-Based Access Control model with Break-The-Glass approach, using contexts and obligations. The new context-based access control model is discussed in Chapter 5.

5. **Prototype Design and Development:** A prototype named CEATH, that is Context- Enhanced Access in a Tanzania Healthcare system, has been designed and implemented in order:

   - To demonstrate the applicability of the new Role and Context-Based Access Control (RoC-BAC) model
   - To examine overheads introduced by incorporation of contexts and obligations into Role and Context-Based Access Control model (using CEATH system) against that of a Role-Based Access Control (RBAC) model (enforced in to EMR-RBAC system)

   In addition to other techniques such as special configuration of Unified Modeling Language (UML), known as SecureUML, Entity-Relationship Model (Chen, 1976) has been used for the conceptual design of the system. With an earlier approach, techniques such as Class and Sequence Diagrams were used to identify require-

ments and for analysing the relationship between modules. Yii framework which requires Java (as a server side scripting language) and MySQL, which is an open-source relational database management system were the main components used to implement the two prototypes, as discussed in Chapter 6.

6. **Evaluation:** The evaluation part of this research was carried out in three phases. Initially, the capabilities of RoC-BAC are compared against other access control models (including DAC, MAC, RBAC and ABAC) based on criteria specified by the National Institute of Standards and Technology (NIST). Further, an evaluation of performance overheads introduced by new elements and relations (that is, contexts and obligations) was performed. Finally, the usability of the CEATH system which implements RoC-BAC model is evaluated by the healthcare professionals in Tanzania. Prototypes for CEATH and EMR-RBAC wwere implemented in two hospitals to allow healthcare professionals to use the system before its usability is measured by System Usability Scale. The discussion on different aspects of evaluation is in Chapter 7.

1.5 Expected Results

This thesis makes a number of contributions to the body of knowledge, including:

1. A generic methodology, named COIL, for gathering comprehensive access control requirements in the healthcare domain is proposed. The COIL methodology is the synthesis of four elements: contexts, organisational rules, electronic healthcare initiatives, and legislative rules. Each of the four components of the COIL methodology has its own impact in relation to access to electronic health records.

2. A taxonomy for classifying access control models is also proposed in this thesis. The

intent of the proposed taxonomy is to identify how existing access control models can be classified against the proposed Role and Context-Based Access Control (RoC-BAC) model.

3. To support the continuity of care in an accountable manner, a new context-based access control model is designed. The Role and Context-Based Access Control model is developed for the healthcare domain, and it is an extension of traditional Role-Based Access Control (RBAC) model with health-related contexts and obligations.

4. With the proposed RoC-BAC model, a new concept of health-related contexts is also introduced. It represents specific contexts from the healthcare domain that should be evaluated by an access control system in order to support the continuity of care.

5. A prototype that implements the Role and Context-Based Access Control model is developed. The prototype, called CEATH (Context-Enhanced Access in a Tanzania Healthcare), was developed in order to achieve two purposes: 1. to demonstrate that RoC-BAC model is feasible and, 2. to evaluate the performance overheads introduced by new entities and relations. Through its support of context-based policies, and especially health-related contexts, it has been demonstrated in this thesis that the incorporation of health-related contexts and obligations helps healthcare professionals to bypass access rules in an accountable manner in case of an infrequent emergency access, which in turn supports the continuity of care.

1.6 Publications

This research has produced a total of twelve publications. That is, one Book Chapter (BP), three Journal Articles (JA) and eight Conference Papers (CP). These publica-

tions are listed here based on their association with three research contributions

1.6.1 Contribution I: Taxonomy of Access Control Models

CP. **Omary, Z.**, Mtenzi, F., and Wu, B. "Taxonomy of Access Control Models for Healthcare Systems" To be submitted in the 7th International Conference on Information Technology (ICIT 2015), Al-Zaytoonah University of Jordan, Amman, Jordan, May 12-15, 2015

1.6.2 Contribution II: COIL

CP. **Omary, Z.**, Mtenzi, F., Wu, B., "Controlling Access to Patients Information using Cases", presented at the International Conference on Information Society (i-Society 2011), London, United Kingdom, June 27- 29, 2011.

CP. **Omary, Z.**, Mtenzi, F., and Wu, B. "Context for Securing EHRs in a Dynamic Healthcare Environment" the 5th International Conference on Information Technology (ICIT'11), Al-Zaytoonah University of Jordan, Amman, Jordan, May 11-13, 2011

1.6.3 Contribution III: RoC-BAC

CP. Omary, Z. Dynamic Context-Aware Access Control Framework for Securing Electronic Healthcare Records in Tanzania: Implementation Approach, Healthcare Informatics Society of Ireland (HISI)15th Annual Conference , Dublin, Ireland, 17-18 Nov 2010

BC. **Omary, Z.**, Mtenzi, F., Wu, B. Context and Access Control for Healthcare Frontiers of Information Technology, MASAUM Networks 2012, ISBN: 978-969-9742-00-2

CP. **Omary, Z.**, Mtenzi, F., Wu, B., "Dynamic Context Aware Access Control Model for the Areas with the Shortage of Healthcare Professionals", International eHealth, Telemedicine and Health ICT Forum for Educational, Networking and Business, ISSN 1998-5509. Editors: Jardanova, M. and Lievens, F. Luxembourg, G.D. of Luxembourg, April 18-20, 2012. pp. 831-835.

1.6.4 Other Publications

The following articles and conference papers related to electronic healthcare and Tanzania healthcare system were also published

CP. **Omary, Z.**, Lupiana, D., Mtenzi, F., and Wu, B. "Challenges to E-Healthcare Adoption in Developing Countries: A Case Study of Tanzania," First International Conference on Networked Digital Technologies (NDT'09), IEEE, pp.201-209, 28-31 July 2009, ISBN: 978-1-4244-4614-8, pp. 201 - 209.

JA. **Omary, Z.**, Lupiana, D., Mtenzi, F., and Wu, B. "Analysis of the Challenges Affecting E-healthcare Adoption in Developing Countries: Case of Tanzania", in the International Journal of Information Studies (IJIS), Volume 2, No. 1, 2010, 38-50.

JA. **Omary, Z.**, Mtenzi, F., and Wu, B. "Politics vs. Electronic Healthcare: Discussion on How Politics Affect E-Healthcare Adoption" in the International Journal of Digital Society (IJDS), ISSN 2040 2570 (Online), Volume 1, Issue 2, 2010.

JA. **Omary, Z.**, Mtenzi, F., Wu, B., and O'Driscoll, C. "Ubiquitous Healthcare Information System: Assessment of its Impacts to Patient's Information" in the International Journal of Information Security Research (IJISR), ISSN: 2024-4639, Volume 1, Issue 3, 2011, 71-77.

CP. **Omary, Z.**, Mtenzi, F., and Wu, B. "Design and Development of a Framework

for Securing E-healthcare Information" The 14th Annual Conference on Healthcare Informatics Society of Ireland (HISI), Dublin, Ireland, 18-19 November 2009.

CP. **Omary, Z.**, Mtenzi, F., and Wu, B. "How does Politics Affects e-Healthcare Adoption" The Fourth International Conference on Internet Technologies and Secured Transactions (ICITST), London, United Kingdom, 9-12 November 2009, ISBN: 978-1-4244-5647-5, pp. 1-8.

CP. **Omary, Z.**, Mtenzi, F., Wu, B., and O' Driscoll, C. "Accessing Sensitive Patient Information in Ubiquitous Healthcare Systems The 5th International Conference on Internet Technologies and Secured Transactions (ICITST 2010)", London, United Kingdom, 8-11, Nov 2010, ISBN: 978-1-4244-8862-9, pp. 1-3.

1.7 Thesis Structure

The remaining chapters of this thesis are organised as follows.

In Chapter 2, the background to the Tanzania's healthcare system is discussed. Among others, this chapter discusses its organisational structure as well as challenges that Tanzania as a country faces, with special consideration on human resources for health. The chapter also discusses the status of electronic healthcare adoption and use in the country.

The traditional access control models which have been implemented in numerous application domains are discussed in Chapter 3. Among others, the Chapter analyses the suitability of traditional access control models in modern healthcare environments, before proposing a taxonomy for classifying access control models.

Chapter 4 discusses the development of a generic methodology for gathering compre-

hensive access control requirements for the healthcare domain. It is a combination of contexts, privacy and security capabilities, legislative and organisational rules. COIL is, in fact, a methodological approach performed to identify a comprehensive list of access control requirements for the healthcare domain.

Chapter 5 discusses the design of context-based access control model named RoC-BAC, which is an abbreviation for Role and Context-Based Access Control. To support the continuity of care by better handling infrequent access requests in an accountable manner, the developed RoC-BAC model is an extension of the well-known and widely adopted traditional Role-Based Access Control (RBAC) model with health-related contexts and obligations. With this model, a new concept named health-related context is also introduced.

The prototype implementations of RBAC and RoC-BAC models are discussed in Chapter 6. While CEATH system was designed and implemented in order to demonstrate that RoC-BAC model is feasible, the EMR-RBAC system which is built from traditional RBAC model is purposely implemented in order to allow the comparison of the two models in terms of their performance as a result of the introduction of new entities and relations.

Chapter 7 discusses an evaluation of the proposed RoC-BAC model against that of a pure RBAC model. In particular, this chapter discusses three distinct ways that RoC-BAC can be evaluated. That is, firstly, based on the criteria specified by NIST that can be used to evaluate access control systems, followed by comparative analysis of the performance of two prototypes that implements RBAC and RoC-BAC. And finally, evaluation of CEATH by healthcare professionals in Tanzania's healthcare system.

Chapter 8 concludes the thesis, summarises its main findings and points out future research work that could be investigated.

Chapter 2

Tanzania Healthcare System

The main contribution from this thesis is a new context-based access control model purposely designed to support the continuity of care by better handling infrequent access requests, in an accountable manner. This research uses Tanzania's healthcare system as a study domain. The chapter begins with a review on country's historical background in Section 2.1 followed by a discussion on healthcare service delivery system in Section 2.2. Section 2.3 examines challenges of the traditional healthcare system against those of a modern healthcare system whereas ICT is used, also known as e-healthcare. The status of e-healthcare adoption in the country is analysed in Section 2.4. Section 2.5 concludes the chapter.

2.1 Background

Tanzania is a country in the east coast of Africa, consisting of Tanzania mainland and Zanzibar archipelago. The country has a total area of 945,454 square kilometres (sq.km), of which 883,954 is land and the remaining 61,500 is inland water. The country shares borders with Kenya and Uganda to the North, Rwanda, Burundi, Democratic Republic of Congo (DRC) and Zambia to the West, and Malawi and Mozambique to the South. There is also a long coast of Indian ocean to the East.

Figure 2.1: A map of Tanzania showing administrative regions
(Source: Tanzania Government)

The data obtained from the 2012 population and housing census indicate that, the country had a total population of 44,929,002 people, of which, 1,303,568 people were residing in Zanzibar and the remaining 43,625,434 people were in Tanzania mainland (NBS, 2012a). Since Tanzania is one of the countries with highest birth rates in the

world (about 39.664 per 1,000 people), it is estimated by the National Bureau of Statistics that its population as of December 2014 was 47, 421, 786 people, and more than 44% of the total population is under the age of fifteen years old (NBS, 2012b).

The population distribution in Tanzania is characterised to be highly uneven. While the majority of the population in Tanzania mainland (about seventy seven percent) resides in the rural areas, the situation is completely different in Zanzibar where its population is predominantly urban (with about sixty percent) (Madulu, 2012; NBS, 2010). This huge difference between rural and urban population distribution between these two parts of the country is due to the fact that Zanzibar is more urbanised than its counterpart (Madulu, 2012).

Table 2.1: Population and Housing Census 1978 - 2012 (Source: NBS, 2012b)

	1978 Census	**1988 Census**	**2002 Census**	**2012 Census**
Tanzania Mainland	17,036, 000	22,584,000	33,462, 000	43,625, 000
Tanzania Zanzibar	476,000	641,000	982,000	1,304,000
Tanzania	17,512,000	23, 225,000	34,444,000	44,929,000

The country is also characterised by an annual population growth rate of 2.7% in Tanzania mainland and 2.8% in Zanzibar. This has been proven by an increase of more than ten million people in ten years, with an average of 87,000 children born every month throughout the country, as shown in Table 2.1. With the current annual population growth rate, the population in Tanzania is expected to double in the next twenty six years (National Bureau of Statistics, 2013).

It is also estimated that Tanzania has a gross national income per capita of $ 860 and life expectancy of sixty one (61) years. With more than sixty percent of the population living below the national poverty line, the country has a high under-five

Table 2.2: Tanzania Statistics (Source: NBS, 2012a)

Total Population (projection in 2014)	47, 421, 786
Gross National Income per Capital ($) 2013	860
Life expectancy at birth (years) 2012	60.9
Probability of dying under Five (per 1000 live birth)	68
Probability of dying between 15 and 60 (M/F) per 1000	456/311
Total annual expenditure on health per capita ($, 2012)	83
Total expenditure on health as % of GDP (2012)	6.0
Total adult literacy rate (%) 2008-2012	73.21
Primary school net enrolment ratio(%) 2008-2011	98.2

mortality rate of about 15.2%. On a positive note, in relation to education, Tanzania has had a remarkable success in reduction of illiteracy since its independence in 1961. From the 2012 population and housing census, Tanzania has recorded a 73.21% of literacy rate among women and men, which is an accomplishment from the 70% illiteracy rate the country inherited at independence in 1961 (NBS, 2010), (NBS, 2012a), (World Health Organisation, 2012c). These statistical figures are summarised in Table 2.2. Subsequent to the background of the country reviewed here, Section 2.2 discusses its healthcare delivery system.

2.2 Health Delivery System

Administratively, Tanzania is divided into 30 regions, of which five are in Zanzibar and the remaining 25 are in Tanzania mainland. Each region is divided further into

districts. The districts are further divided into divisions, and divisions into local wards and sheshias (in Zanzibar), as presented in Table 2.3. Wards are divided further into villages and streets for rural and urban areas respectively (Othman *et al.*, 2003). In 2012, the government of the United Republic of Tanzania created four new regions and nineteen districts, which brings a total administrative districts to 143, of which 133 are in Tanzania mainland and 10 are in Zanzibar (Prime Minister's Office RALG, 2012), (NBS, 2013).

Table 2.3: Tanzania administrative divisions (Source: National Bureau of Statistics (2009), Prime Minister's Office RALG (2012)

	ZANZIBAR	TANZANIA Mainland	TOTAL
Regions	5	25	30
Districts	10	133	143
Divisions	20	516	536
Local Wards and Sheshias	332	2,542	2, 874

The current healthcare delivery system in Tanzania was established upon independence in 1961 following colonial, urban and curative-based healthcare system from earlier colonial regimes. Contrary to colonial governments in numerous cities, such as Madras (currently known as Chennai, India), which encouraged private-for-profit healthcare services by offering subsidies to healthcare practitioners (Mills, 1998), in Tanzania, however, the overall healthcare system was characterised by little equity and accessibility to the population as a whole. During the colonial period, "proper doctoring" was only confined to British citizens and there were only 12 medical doctors out of 120 Tanzanian with university degrees (Gish, 1973).

After independence in 1961, the government provided free medical services to all citizens and private-for-profit medical practice was banned. In the late 1960s, the post-

colonial government through the Ministry of Health and Social Welfare (MoHSW) began to expand healthcare services, infrastructure and other resources to the rural areas, which was also associated with implementation of various policies and strategies. One among the popular policies developed by the government at the time emphasized on equitable distribution and access to healthcare resources and services (MoHSW, 1990). The government also set a strategy to train indigenous practitioners. Based on these policies and strategies, a large number of medical doctors were trained, and healthcare services were offered free of charge in all public health facilities (Abel-Smith & Rawal, 1992).

As part of economic recovery and structural adjustment, the government of the United Republic of Tanzania introduced the regulated private practice in 1991 and the cost sharing policy in all public health facilities in July 1993. This latter policy aimed to improve efficiency and to foster sustainability in the provision of healthcare services through community participation (Munishi, 1997). To enable citizens to get familiar with the newly introduced policy and also to control flow of patients to referral and consultant hospitals, the MoHSW introduced user charges in two distinct phases. The charges were first introduced in referral and consultant hospitals, whereby anyone visiting a referral hospital was required to pay, and later the charges were introduced for patients attending health centres and dispensaries. As part of the policy, there were also automatic waivers and exemptions granted to specific services, groups and diseases such as all maternity services, children under five and specific (including tuberculosis and leprosy) and chronic diseases that would drain a substantial amount of income if patients would be asked to pay. Although healthcare as a service has evolved since independence, there are still some geographical inequalities in relation to access to healthcare services in the country. With development and the availability of opportunities, some regions of the country tend to attract more healthcare professionals that others.

There are also some positive changes that characterise the Tanzania's healthcare system. First and foremost, today's healthcare system is marked by a reform and improvement. There has been an expansion of healthcare services in rural areas facilitating greater access to the rural population. And the majority of the population currently lives within five kilometres of a healthcare facility, which is an improvement compared to more than 90 percent living within 10 kilometres in the 1980s (MoHSW, 2003), (National Bureau of Statistics, 2009). The doctor population ratio has also improved to 1: 30,000 from 1:50,000 in 2006 (Manzi *et al.*, 2012). Despite the improvement, this ratio is still low compared to 2.7 and 2.8 doctors per 1,000 people in Ireland and United Kingdom respectively (World Bank, 2015) and the recommended rate of 1:1000 doctor to population ratio and 1:7,500 dentist to population ratio for developing countries by the World Health Organisation (WHO) (Kinfu *et al.*, 2009).

Table 2.4: Tanzania Health Statistics in 1961 (Source: Kinfu *et al.*, 2009)

Total Population	10, 400,000
Birth rate per 1000 population	49.3
Death rate per 1000 population	20.3
Life expectancy	44
Under 5 mortality rate per 1000 population	240

The low doctor to population ratio is due to numerous reasons including fast growing population and low student registrations in medical schools among others (Mkony, 2010). The ratios for pharmacists, dentists, nurses and other healthcare professionals are exceedingly low by international comparison (Manzi *et al.*, 2012). Table 2.4 shows other health statistics in Tanzania in 1961. These and other characteristics of the Tanzania healthcare system that might affect the continuity of care are discussed

further in Section 2.2.2.

2.2.1 Referral Health System

The healthcare services in Tanzania are offered by a number of institutions through a referral system that is categorised into different levels, ranging from community level to treatment abroad. The healthcare institutions forming a referral structure include dispensaries, health centres, district hospitals, regional hospitals and, referral and consultation hospitals, as shown in Figure 2.2.

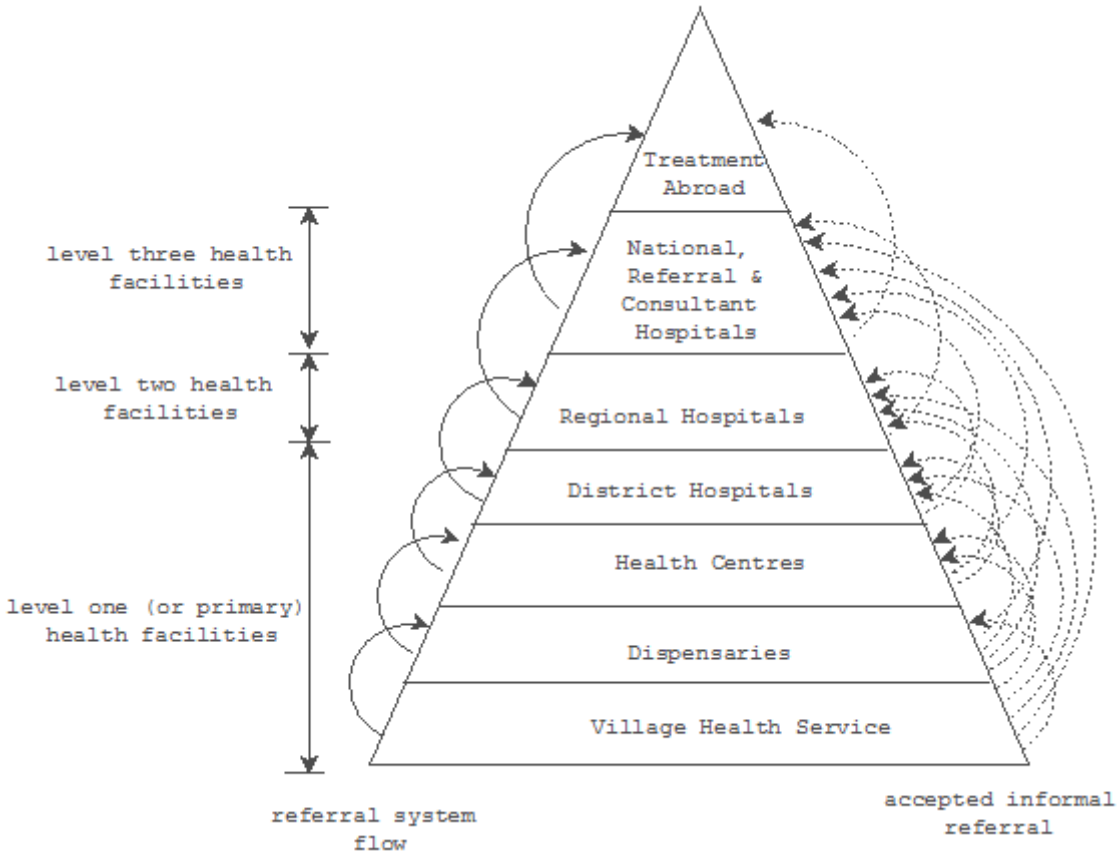


Figure 2.2: The referral structure of the Tanzania healthcare system (Source: Author)

As pointed out by the World Health Organisation (2008), an effective referral system

ensures a close relationship between all levels of the health system and helps to ensure that people receive the best possible care closest to home. It also assists in making cost-effective use of hospitals and primary health care services. Additionally, a referral system should be able to offer support to health centres and other primary health care providers by experienced staff from district and regional hospitals. This in turn helps build capacity and enhances access to better quality care.

Despite a long list of proven benefits of a referral health system, the Tanzania's health-care system is characterised with an acceptable informal referrals that affect the efficiency and effectiveness of the overall healthcare system. It is actually common for patients to seek healthcare services in secondary health facilities, including district and regional hospitals, without being referred by a primary care health facility such as a dispensary or a health centre. This practice results in i. patients receiving optimal care not at the appropriate level, which could be costly ii. secondary health facilities not being used cost-effectively, iii. patients who mostly need specialist health services cannot access them in a timely manner and iv. primary health care facilities being under utilized (World Health Organisation, 2008). The acceptable informal referrals in a Tanzania's healthcare system are indicated by dotted lines in Figure 2.2.

This section reviews each of the units responsible for providing health care services in Tanzania mainland as discussed in its national health policies: MoHSW (1990), MoHSW (2003), and MoHSW (2007).

Village Health Service: To ensure that each individual or household takes care of its own health, the government of the United Republic of Tanzania established a village health post to all villages without a health facility in 1990 (MoHSW, 1990). The village health post is the lowest level of health care delivery in the country, and it is offered at the community level. It offers preventive services which could be provided at homes. Usually, the village health post does not require a permanent building

to offer its services but rather only an office is required for storage of medicine and equipment. Two village health workers are required for each village health facility, one who will deal with maternal child problems and the other will deal with environmental sanitation. The village health workers are chosen by the village government amongst the villagers and are given a short training before they can start providing services to citizens.

The health services offered at the village or community level include

- Health education about diseases in the community
- Health education about clean and safe water, hygiene and environmental sanitation
- Advice on food and nutrition and, maternal and child health
- Collection of statistics on diseases and immunisations, and
- Treatment of minor ailments

Dispensaries: This is the first formal level-one health care unit in the country, providing comprehensive primary health care services to citizens. Each dispensary is expected to serve between 6,000 and 10,000 people, and to supervise all the village health workers in its ward. A dispensary is staffed by a clinical assistant, with one or two helpers: a public health nurse or a nurse midwife and a rural health assistant (NBS, 2012b). The clinical assistants usually receive a three year course of training in anatomy, physiology and hygiene with good grounding in diagnostic methods and treatment of common diseases.

The following are some of the health care services offered by dispensaries:

- Health education to people served by the dispensary
- Maternal and child health and delivery services

- Treatments and immunization services to children
- Treatment of diseases
- Continuation of treatment for tuberculosis, mental and other diseases in collaboration with higher level health facilities
- Health care services and health education to schools
- Conduct visits to villages for the purpose of identifying health problems and trying to solve them or refer to higher health facility
- Provide expertise and supervision to village health workers in the villages served by the dispensary
- Refer patients with complicated conditions to higher-level health facilities, especially health centres

Health Centres: This is the second formal level-one health care service delivery unit in Tanzania, supporting dispensaries and are expected to serve about 50,000 people. Although, health centres give priority to preventive measures and hygiene, they are, however, extensively used for treatment of common diseases. Each health centre is run by a clinical officer with a secondary school education and more elaborate education in diagnosis, treatment and minor surgery (NBS, 2012b). The clinical officer running a health centre is usually assisted by one or two clinical assistants, a nurse or a nurse midwife with one or two child health aids, a health aid and a health assistant.

Health centres offer similar services to those offered by the dispensary but with more sophisticated services. These include

- In-patient department with 20-30 beds for patients who require short hospitalization

- Supervision of dispensaries as well as provision of primary health care services in the division

District Hospitals: The district is a crucial level in the provision of health care services in the country. Each district is expected to have a district hospital serving about 250,000 people. For those districts which do not have government hospitals, the government usually negotiates with religious organisations to designate voluntary hospitals as district hospitals. The district hospital contains a mixture of qualified staff with different specialities, including: graduate and assistant medical officers, nurses of different qualifications, pharmacists, laboratory technicians, radiologists, health officers and health secretaries. The health services offered at district hospitals include the following:

- Conducting on-job training for all medical staff in the district
- Identifying major health problems in the district and working out strategies to overcome them
- Conducting operational research aimed at providing efficient health services in the district
- Participating in the training of health staff of the district hospital
- Referring patients who require special treatment to regional hospitals

Regional Hospital: This is a hospital establishment providing level two referral hospitals from level one hospitals, that is district hospitals. They are responsible for providing health care services in a region. As of 2012 figures from the National Bureau of Statistics (NBS), there were about eighteen regional hospitals in the country (NBS, 2012b). The regional hospital offers the following functions

- Provides all services offered at the district level but at the higher level of expertise

(and more staff, with about 5-10 doctors and 1-2 consultants)

- Offers second level referral services from level one hospitals
- Conducts teaching and training of middle and operational level health cadre, including clinical assistants and nurses
- Conducts health research programs including operational research of health systems research in the region
- Provides technical skills to lower health facilities in the region and offer specialised treatment in medicine, surgery, obstetrics and gynaecology and paediatric.

National, Referral and Consultant Hospitals: This is level three and the highest level of health care services delivery in the country. As its name suggests, the national, referral and consultant hospitals act as referral centres for level two hospitals.

- **National Hospital:** The Muhimbili National Hospital (MNH) is the only national hospital in the country, supervised by the Ministry of Health and Social Welfare (MoHSW). It also acts as the zonal referral hospital for the Eastern Zone.
- **Zones for Referral Hospitals:** Currently, there are four sophisticated zonal referral and consultant hospitals in the country. These are Muhimbili National Hospital (MNH), two voluntary agency hospitals (Bugando Medical Centre (BMC) and Kilimanjaro Christian Medical Centre (KCMC)) and Mbeya Hospital, which is owned by the government. These referral hospitals are located on the Eastern, Western, Northern and Southern Highlands zones respectively. Referral hospitals are equipped with a mix of qualified specialists and consultants as well as sophisticated modern medical equipments so that to allow healthcare professionals are able to handle cases which would otherwise be referred abroad.

The referral hospitals offer the following services:

  - All the medical services offered at the level two health facilities but at a specialist level
  - Conducts the training of high and middle level health personnel
  - Teaching undergraduate and postgraduate medical students plus other allied courses
  - Conducts research in the medical field
  - Conducts outreach visits to other hospitals in the zone to offer specialists support services to the medical staff

- **Specialised Hospitals:** There are two specialised hospitals in Tanzania mainland. These are, Mirembe Hospital (in Dodoma) and Kibongoto (in Moshi) providing health care services to mentally ill and tuberculosis patients respectively. These hospitals are directly supervised by the Ministry of Health and Social Welfare (MoHSW) and, are equipped with qualified specialists and consultants as well as sophisticated modern medical equipment to allow healthcare professionals to deliver health services as needed.

Treatment Abroad: For health care services that are not available in Tanzania, patients are referred abroad for treatment on government subsidy.

The health facilities in Tanzania may also be categorised based on ownership. That is, health facilities owned by the government (also known as public hospitals or public health facilities), and those owned by non-government organisations such as those owned by parastatal organisations, religious institutions and private organisations. As summarised in Table 2.5, by September 2014, Tanzania mainland had a total of 6,270 health facilities. Of these, 4,739 are government owned and the remaining

Table 2.5: Number of health facilities in Tanzania (Source: MoHSW, 2013b)

Type of Facility	Government Owned		Non-Government Owned		Total Facilities	
	YEAR					
	2013	2014	2013	2014	2013	2014
Dispensaries	3,099	4,219	1,312	1,259	4,411	5,478
Health Centres	336	416	126	158	462	574
Hospitals	70	104	109	114	179	218
Total	3,505	4,739	1,547	1,531	5,052	6,270

1,531 are owned by non-government organisations. For government owned health facilities, there are 4,219 dispensaries, 416 health centres and 104 hospitals. With non-government health facilities, there are 1,259 dispensaries, 158 health centres and 114 hospitals. From these statistics, it can be noted that dispensaries occupy 88% of all health facilities, followed by health centres that account for 9% and hospitals constitutes only 3%. Section 2.2.2 discusses the status of human resources for health in the Tanzania's healthcare sector.

2.2.2 Health Workforce

The statistics on human resources for health show that the number of qualified health workers in Tanzania have declined in absolute numbers relative to the size of the population. The shortage began in 1990s when the government retrenched health workforce and imposed an employment freeze, resulting into a loss of about one third of health workers. Within ten years, between 1995 and 2005, out of 23,474 university graduates, the government employed only 3,036 healthcare workers, which is about 16 per cent of the overall graduates. Even now, the number of graduates from medical schools employed by the government is still very low.

In 2006, the Ministry of Health and Social Welfare (MoHSW) reported that, there were

about 29,000 staff working in government-owned health facilities (with an estimate of 65% shortage) and about 6,000 staff working in private hospitals (with an estimate of 86% shortage). To meet the demanding needs of the health system, the ministry estimated that an additional of 144,700 health workers would have to be trained and employed to work in government-owned health facilities and another 39,400 for non-government facilities. Tables 2.6 and 2.7 summarises the shortage of health workers for both private and public health facilities in Tanzania.

Table 2.6: The Status of Human Resources for Health in Private Health Facilities (Source: MoHSW, 2008a)

Facility Level	**Available Health Facilities**	**Health Workers**				**Staff Shortage %**
		Required Staff per Establishment 2005	**Required Staff for Existing Facilities**	**Available Staff 2006**	**Staff Shortage 2006**	
Hospitals	132	197	26, 004	3, 251	22, 753	87.5
Health Centres	150	36	5, 400	758	4, 642	86.0
Dispensaries	1, 641	7	11, 487	1, 842	9, 645	84.0
Training Institutions	36	*	756	288	468	61.9
TOTAL	**1, 959**		**43, 647**	**6, 139**	**37, 508**	**85.9**
Attrition Rate 0.5% per year					**1, 875**	
TOTAL NEW STAFF REQUIRED FOR PRIVATE HEALTH FACILITIES					**39, 383**	

* indicates health facilities or institutions with varying staffing level

Table 2.7: Human resources status in Government-Owned Health Facilities (Source: MoHSW, 2008a)

Facility Level	**Health Facility**			**Health Staff**						**Required Staff to fill the existing Gaps**
	Available Facilities 2006	**New Facilities 2007–2017**	**Total**	**Required per Establishment 2005**	**Required for Existing Facilities**	**Medical Professionals Available 2005**	**Shortage 2006**	**Shortage %**	**PHSDP Requirement 2007-2017**	
Referral and Specialised Hospitals	8	–	8	*	8, 546	4, 477	4, 069	48	–	4, 069
Regional Hospitals	21	–	21	346	7, 266	2, 481	4, 785	66	–	4, 785
District Hospitals	95	19	114	197	22, 458	7, 364	15, 094	67	3, 743	18, 837
Health Centres	331	2, 074	2, 405	36	11, 916	4, 908	7, 008	59	49, 776	56, 784
Dispensaries	3, 038	3, 108	6, 146	10	30, 380	9, 384	20, 996	69	31, 080	52, 076
Training Institutions	72	4	76	*	1, 711	449	1, 262	74	–	1, 262
Total	**3, 565**	**5, 205**	**8, 770**	–	**82, 277**	**29, 063**	**3, 214**	**65**	**84, 599**	**137, 813**
						Attrition Rate 0.5% per year			**4, 230**	**6, 891**
									88, 829	**144, 704**
TOTAL NEW STAFF REQUIRED (2007-2017)									**88, 829**	**144, 704**

* indicates health facilities or institutions with varying staffing levels

Table 2.8: Student enrolment by major fields and level of study (Source: SARUA, 2011)

Major Field of Study	**Number of students enrolment**				
	Undergraduate	PG Dip.	Master	Doctoral	Post Doctoral
Agriculture	640	0	101	10	0
Business, Management and Law	9935	1035	2528	24	0
Education	14,569	61	96	1	0
Human Sciences	1628	0	302	4	1
Humanities and Social Sciences	11596	877	599	16	0
Science, Engineering and Technology	7852	607	202	44	0

The human resources situation in the healthcare sector in Tanzania is in severe crisis, according to statistics presented in Table 2.6 and 2.7 and also from a report by the World Health Organisation (WHO). In its recent report, the World Health Organisation (2013a) estimates the global shortage of 7.2 million health workers, with 83 countries Tanzania inclusive facing an acute shortage of healthcare workers from community level to qualified ones including doctors, specialists, nurses and other professionals. The reasons behind such a crisis include poverty, migration of health workers to industrialised countries (brain drain), poor governance, poor living and working conditions, and retirement and deaths of health workers. There is also internal migration of health workers out of general health services to horizontal health programmes, as a result of low salaries and overwork.

In comparison to the other fields of study, there is also a low capacity of enrolment in medicine in Tanzania. For the year 2011, for instance, the Tanzania Commission for Universities (TCU) enrolled a grand total of 135,367 students, of which 92,977 were enrolled in public universities and the remaining 42,390 in private universities (NBS,

Table 2.9: Medical Doctor First Year Enrolment Capacity for Different Universities in Tanzania (Source: TCU, 2012)

University Name	Capacity for First Year Medical Doctor Enrolment
Muhimbili University of Health and Allied Sciences (MUHAS)	200
International Medical & Technological University (IMTU)	180
Catholic University of Health and Allied Sciences (CUHAS)	150
Kilimanjaro Christian Medical College (KCMC)	150
University of Dodoma	120
Hurbert Kairuki Memorial University	50
Saint Francis University	50
Total	900

2013). With sample data of students enrolment based on major fields and level of study presented in Table 2.8. While Education and Human Sciences enrolled 14,569 and 11,596 undergraduate students respectively (SARUA, 2011), medicine is capable to enrol only 900 medical degrees students in a year across seven universities, as shown in Table 2.9.

The ratio of health workers per population in a Tanzania healthcare system is still far below the rate recommended by the World Health Organisation (WHO), that is 22.8 doctors, nurses and midwives per 10,000 population. The 2013 statistics from the MoHSW (2013), and sample data presented in Table 2.10, indicate that there was a total of 346 medical specialists and consultants, 1,135 medical doctors working in different parts of the country and 14,096 nurses and nurse midwives. These ratios

Table 2.10: Health Workers per Population Ratios at National Level (per 10,000 Population) (Source: MoHSW, 2013)

Profession	Total	HRH per 10,000 Population
Medical Specialists and Consultants	346	0.079
Medical Doctor	1,135	0.260
Nurse and Nurse Midwives	14,096	3.231
Medical Attendants	19,666	4.508
Assistant Medical Officer	1,741	0.399
Assistant Nursing Officer	4,248	0.974

equal 0.079 medical specialists and consultants, 0.0260 medical doctors and 3.231 nurses and nurse midwives for every 10,000 population. Similar to skilled health workers, the ratios are also low for the supporting workers.

Despite the government's effort to establish strategies and policies that aim to reduce the low ratio between health workers and population (especially in rural areas), the region-wise distribution is highly uneven. As depicted in Table 2.11, Dar es Salaam has a total population 4,364,541 that can be served by 223 medical doctors, Manyara has 1,425,131 people and 21 medical doctors, and Kigoma has 2,127,930 and 16 medical doctors. From these statistics, one medical doctor is expected to serve a population of 19,572 in Dar es Salaam, 67,863 in Manyara and 138,620 in Kigoma (MoHSW, 2013). Furthermore, out of 16 medical consultants in the country, 11 works in Mwanza, 3 in Arusha and 2 in Kilimanjaro. There are various reasons that influence health workers' area of choice of practice resulting into uneven region-wise distribution. These may include future career plan, better living and working conditions and the availability of private health facilities that would allow public health workers to engage in private

Table 2.11: The distribution of health workers in selected regions in a Tanzania) (Source: MoHSW, 2013)

No.	Region	Population	Medical Consultants	Medical Specialists	Medical Doctors	Nurses & Nurse Midwives
1.	Dar es Salaam	4,364,541	-	141	223	1,274
2.	Kilimanjaro	1,640,087	2	32	91	1,065
3.	Iringa	941,238	-	4	52	1,011
4.	Mbeya	2,707,410	-	11	128	1,211
5.	Mwanza	2,772,509	11	58	128	1,179
6.	Kagera	2,458,023	-	1	26	788
7.	Arusha	1,694,310	3	6	45	425
8.	Mtwara	1,270,854	-	1	24	350
9.	Kigoma	2,127,930	-	2	16	414
10.	Manyara	1,425,131	-	3	21	385
11.	Rukwa	1,004,539	-	2	17	332
12.	Pwani	1,098,668	-	6	32	314

- indicates no health worker in the region

health work.

In addition to the shortage of health workers, the Tanzania's healthcare system is characterised by an increasing number of patients, as shown in Table 2.12. For the year 2008, for instance, there was a total of 36,425,330 outpatients who received treatment from various health facilities throughout the country. Among them, 5% received treatment in hospitals, 13% in health centres and the remaining 82% in dispensaries, as summarised in Table 2.12. Looking at the regional distribution of medical consultants, specialists and doctors, a 2013 report published by the MoHSW (2013) noted that, 68% of all medical consultants were based in Mwanza, 47% of medical specialists and 20% of all medical doctors were working in Dar es Salaam. Out of a total of 64, 449 health workers, only 32,036 are considered to be serving the

Table 2.12: Number of patients treated annually in Tanzania mainland between 2000 and 2009 (Source: MoHSW, published by the NBS (2012b))

Year	Outpatients			Inpatients
	Hospitals	Dispensaries	Health Centres	
2000	989, 101	13, 697, 988	1, 874, 346	626, 700
2001	1, 167, 139	17, 218, 371	2, 511, 624	680, 263
2002	1, 328, 395	19, 695, 356	3, 258, 520	701, 568
2003	1, 491, 909	22, 935, 688	3, 659, 615	1, 390, 273
2004	1, 532, 028	23, 552, 460	3, 758, 027	2, 125, 388
2005	1, 619, 700	24, 900, 276	3, 973, 085	2, 237, 146
2006	1, 754, 925	26, 976, 136	4, 304, 787	2, 837, 252
2007	1, 842, 671	28, 328, 093	4, 520, 026	2, 979, 115
2008	1, 934, 805	29, 744, 498	4, 746, 027	3, 128, 071
2009	1, 128, 286	32, 718, 948	5, 220, 630	3, 440, 870

rural population which is about 75% of the total population (MoHSW, 2013). For the medical doctors, Dar es Salaam has a high ratio of about one medical doctor per 20,000 population, compared to the national average of 3.5:100,000. These ratios are low compared to 2.7 and 2.8 medical doctors per 1000 population in Ireland and United Kingdom respectively and an average of 3.4 medical doctors per 1000 population in Europe (World Bank, 2014). The regional distribution of hospitals in Tanzania is presented in Table 2.13.

As a result of a shortage in human resources for health, it is common to find mid-level health workers performing basic health care jobs that were meant for skilled health workers in order to support the continuity of care. This thesis, therefore, supports

Table 2.13: The regional distribution of health facilities in Tanzania) (Source: MoHSW, 2013)

No.	Region	Designated District Hospital	National	Private	Public	Regional	Regional or Zonal	Specialist	Faith-Based	Zonal	Total
1.	Dar es Salaam		1	16	4	5		2	3		40
2.	Kilimanjaro	5		3	3	1		1	4	1	18
3.	Iringa	3		3	4			1	4		18
4.	Mbeya	2		2	6	1			6	1	18
5.	Mwanza	2		4	5	1			2	1	17
6.	Kagera	5		1	3	1			6		16
7.	Arusha	3		3	4	1			4		15
8.	Mtwara				1		1		1		3
9.	Kigoma	1			2	1			4		8
10.	Manyara	1			3	1			2		7
11.	Rukwa	2			1	1					4
12.	Pwani				5	1			1		7
13.	Dodoma	1			3		1	1	2		8
14.	Lindi	1			4	1			2		9
15.	Morogoro	4		1		1			2		13
16.	Mara	4		1	1	1			2		9
17.	Ruvuma	1		1	2	1			4		10
18.	Shinyanga	1		2	4	1					9
19.	Singida	1			2	1			5		9
20.	Tabora	1			3	1			2		7
21.	Tanga	2		2	4	1			4		13
	Total	41	1	39	64	23	2	4	60	3	237

the existing approach to health care service delivery by proposing a new context-based access control model that allows healthcare professionals to access patients' information in an accountable manner in case of infrequent emergency. The proposed access control solution addresses the shortage of qualified health workers at all levels of the healthcare system in Tanzania.

2.3 Traditional Health System

This section provides a discussion on the issues facing the Tanzania's healthcare system as a result of its partial implementation of electronic medical records. The section is divided into three parts: Section 2.3.1 discusses what a traditional health system is, Section 2.3.2 analyses issues associated with traditional health system in terms of the type of medical records supported and used, and Section 2.3.3 discusses the benefits of e-healthcare adoption and use.

2.3.1 Introduction

Barely in use before 1999, electronic healthcare or e-healthcare has now become a topical *"buzzword"* used to characterise the usage of ICT in the health care industry (Sharma *et al.*, 2006), (Omary *et al.*, 2009). Electronic healthcare has flourished in the past decade due to limitations imposed by traditional health care service delivery which uses traditional "paper-based" medical records. In this thesis, a traditional medical record is defined as a "paper-based repository of patient information that is reviewed or used by the health provider for either clinical, research or financial purposes" (Harman *et al.*, 2012). These records are used by skilled health workers, such as medical doctors and medical specialists, to manually record patient's medications and tests on every patient's visit to the healthcare facility. More commonly, they are known as "paper charts", and each unit of the hospital has the responsibility to maintain its own set of records for each patient.

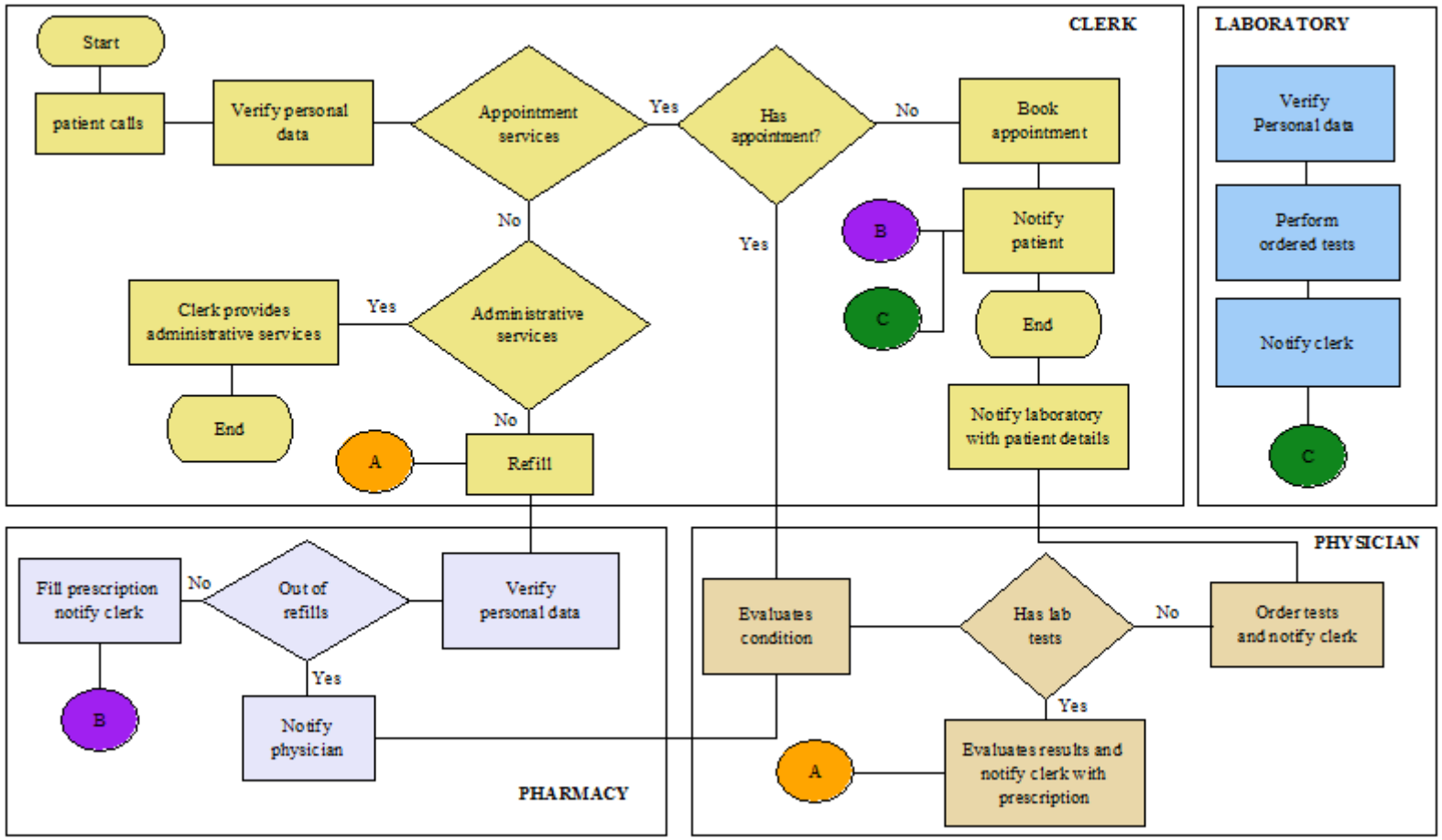


Figure 2.3: Flow Chart for Traditional Medical Record System (Source: Krishna, 2010)

To provide a thorough understanding of the risks and disadvantages of traditional medical record systems, this thesis uses a scenario from Krishna (2010), depicted in Figure 2.3, to show how these records work in the provision of care.

The process begins when a patient visits a hospital and an assistant (labelled "clerk") asks a patient for his personal information. Based on the information provided by the patient, an assistant retrieves the respective medical record from existing storage (whether paper file or computerised file system). After records have been retrieved, the patient may then request one or more health services. These may include: appointment with the physician (same as a medical doctor in case of a Tanzania healthcare system), a prescription refill from the pharmacy or any other administrative service. If a patient requests to see a physician, an assistant first checks whether that patient has an appointment or not. If there is no appointment, the assistant then books a new appointment and notifies the patient. If an appointment exists, an assistant notifies the physician about the appointment with the patient.

Upon meeting a patient, the physician evaluates the patient's condition and determines whether there is a need for the requested tests or not. If tests are needed, the physician then passes this information to an assistant using traditional communication methods such as "phone, fax or post (which includes a messenger)". The assistant then notifies a laboratory with the patient's details and list of tests ordered by the physician. Upon arriving for tests in the laboratory, the patient is asked again by a pharmacist for personal information in order to verify what that particular patient is saying against information received from the physician, through an assistant. Usually, this verification procedure is done before any tests are made. When the laboratory test results are ready, they are passed to an assistant, who in turn passes them to the physician. The physician then prescribes the patient's necessary medications after verifying complete medical records. The prescription note is sent to the assistant who

will send it to the pharmacy using traditional communication methods. The pharmacist prepares medication from the prescription note received and then notifies the assistant who will notify the respective patient.

Similarly, when a patient requests a prescription refill, an assistant notifies the pharmacy, the patient information is then verified and a pharmacist checks if that patient has any refills for prescription. When the medication is ready, the pharmacist notifies an assistant whose responsibility is to notify the patient. If no refills are found, the pharmacist notifies the physician.

2.3.2 Challenges of the Traditional Health System

There are various limitations of a traditional paper-based medical record system that have led to the movement to electronic medical records. Among the generic challenges that do not only affect the traditional paper-based medical record system include:

Ambiguity: Since recording of patient information in many hospitals in Tanzania are on paper and thus referred to as paper-based medical records, Gillies (2006) identifies limitations associated with these type of records. Among others, paper-based medical records are characterised with the following features: i. the handwriting may be illegible or long-winded; and abbreviations may vary ii. it is hard to tell whether data items are temporarily missing, misfiled or will never be available, and iii. the language used can be ambiguous (Wyatt & Wright, 1998). The illegible handwriting, for instance, has been identified as a major source of adverse events, not just for doctors. As argued by Lærum *et al.* (2001), these issues of paper-based medical records tend to impede the continuity and quality of care to patients.

Fragmented Records: Depending on a particular need, it is common for patients to visit healthcare providers who are geographically separated from one another. A

patient may visit a General Practitioner (GP) for general health services, a physiotherapist when experiencing physical problems and a psychologist for psychiatric issues. These healthcare providers may be within one single large hospital or healthcare providers located in different areas from one another, outside the hospital. In a traditional healthcare system, each provider is expected to maintain its own records and also to update its copy of records whenever a patient pays a visit. The fragmented medical records in a traditional health system become a challenge when a patient decides to change healthcare provider, and a new provider is required to look for information regarding previous health conditions and treatments so as to create a new set of records. As pointed out by Schoenberg & Safran (2000) and McClellan (2009), it is not easy to retrieve such records in a traditional system.

Limited Accessibility: An access to patient's medical records in a traditional health system is limited to one individual at a time, and only possible on-site where access is requested (Rindfleisch, 1997). The difficulty in accessing and retrieving such records increases when a patient receives treatment from more than one department (say, hypertension and orthopaedic) in a single large hospital. When a patient's paper file is in the hypertension clinic and the patient is currently in the orthopaedic department for check-up, the latter department has to wait until that file is released. This act can be fatal, sometimes leading to death.

Lack of Support to Unexpected or Infrequent Access: A traditional paper-based system requires a lot of space that costs hospitals an enormous amount of money to store and maintain medical records. Regardless of hospital spending, the traditional system on the other hand works very poorly for unexpected or infrequent access requests, such as emergencies, that are common in the healthcare domain since doctors cannot start patients diagnosis and treatment unless medical records are available (Chen & Zhong, 2012), (Fernández-Alemán *et al.*, 2013). In addition, traditional

medical records are characterised with limited locked storage, and anyone can access them without being held accountable. In other words, the traditional medical records are associated with the lack of accountability, confidentiality and security.

Error-Prone Data Exchange: In a traditional medical record system, data is mainly exchanged through paper-based forms, calls, faxes, and even post (through a messenger) (Liu, 2010). These traditional methods are very insecure. As pointed out in Section 2.3.1, for every laboratory test required and medication prescribed, a physician has to pass information to an assistant who is responsible for notifying the laboratory and pharmacy respectively. When laboratory tests or prescriptions are ready, a laboratory technician and pharmacist are required to notify an assistant who will then notify the patient. That being said, the overall flow of information in a traditional paper-based medical system is slow, and error-prone since human beings are involved directly with data exchange.

Labour-Intensive Data Storage and Retrieval: There is a wide range of data types and formats that are gathered, stored, retrieved and shared in healthcare, including x-rays pictures, blood works and CT-Scan reports. First and foremost, paper-based records are stored in bulk and vulnerable to damage from wear and tear, fire, water and coffee spilling. Based on the type of medical records stored, it is difficult to maintain a single file with all of the data types. Similarly, the whole process of data storage and retrieval is labour intensive to hospital staff (either an assistant or a medical doctor). Consider, for instance, the level of difficulty in storage and retrieval that arises from a patient who has been receiving care from the same hospital for five years. The first challenge is, the hospital will have all the information in a single file. When a medical doctor needs to compare patient diseases for the past three years for instance, an assistant has to go through the whole file and retrieve all the data required. After records have been analysed by the medical doctor, which is

time consuming and even error-prone, an assistant has to re-file every single piece of information as it was before retrieval (Miller & Sim, 2004).

High Cost in Care Delivery: Tanzania is one of the countries relatively with low per capita spending on health. While World Health Organisation (WHO) recommends $54 as a per capital health spending, its spending per person is $15.75, as outlined in the third Health Sector Strategic Plan (HSSP III) (MoHSW, 2009). To minimise health care costs and to improve the quality of care delivered, Tanzania is in the initial stages of an implementation of a national e-health information system that is expected to reduce costs in care delivery (MoHSW, 2013c).

2.3.3 Benefits from E-healthcare Adoption

The adoption and use of e-health information systems promise to offer a wide range of benefits to the government, healthcare providers as well as citizens. This section briefly discusses the advantages of e-healthcare.

- **Life Saving:** Too often people neglect their screenings and tests that could even lead to death. Contrary to a traditional paper-based medical system, the electronic health system is capable of sending appropriate alerts and reminders to notify a physician about a screening or test for a certain patient under his care. This ability of an electronic health system is only possible as a result of a patient's basic information (such as age, gender, and family history) being compared against a database of best practices.

- **Quality of Care:** There are two main ways through which electronic healthcare are sought to improve the quality of care. These are:

  - Health web portals: Despite the dangers involved, one of the most signifi-

cant and growing uses of the Internet in healthcare is the availability of websites that contain and allow people to search for health and health-related information, thus improving their knowledge regarding healthy lifestyles, health and self-treatment. The health web portals can also be used by healthcare professionals to search for health-related information purposely for education and research.

- Collaboration: Two healthcare professionals located in two geographically separated areas may collaborate with one another through video conferencing to discuss issues pertaining to a particular medical case. Although considered theoretically feasible, this knowledge sharing approach, however, is difficult to achieve due to the nature of physicians' work as well as privacy, security and confidentiality concerning patient information.

- **Improved Physician's Efficiency:** In his article titled"What is e-health?", Eysenbach (2001) highlights ten promissory $e^{'}$s in e-healthcare, where efficiency is one of them. Other $e^{'}$s stands for "Enhancing" quality of care, "Evidence-based" care, "Empowerment" of patients through knowledge bases of medical information, "Encouragement" of a new relationship between patient and healthcare professional(s) and "Education" of physicians through online sources. The list also includes "Enabling" of information exchange and communication, "Extending" the scope of care beyond domain's conventional boundaries, "Ethics" and, "Equity" between the *haves* and *have-nots*.

  Using a scenario discussed in Section 2.3.1, every time a patient visits a health facility in a traditional paper-based medical system, the patient is supposed to provide personal information and a suggestive symptoms before any services are offered. Since legible and complete electronic medical records are readily available for immediate access at any given point of time, the physician responsible

will already have information about the type of medications that patient is taking or has taken previously, laboratory test results and even allergies. This, in fact, reduces waiting time dramatically and improves the quality of treatment by offering more meaningful interactions between the physician and patients.

- **Physician-Patient Relationship:** With its ability to allow inexpensive retrieval of patient information from anywhere and at anytime, electronic health records are already redefining the physician-patient relationship resulting from sensitive information that is being shared between patients and physicians. In particular, through EHRs, a physician gains a capability to know all health information about his patient from the patient's body to the state of health (Ball & Lillis, 2001).

- **Reduced Expenses:** There are numerous ways that healthcare providers and the government may reduce expenses through adoption of e-healthcare. These include:

  - There is an existence of digital imaging services that can virtually eliminate the need for films and x-rays. A radiology department in a healthcare organisation with an electronic healthcare information system in place can send digital x-ray films to physician's smart phone or any other hand-held devices.

  - Costs can also be reduced by cutting back on unnecessary tests and treatments. Although not discussed in detail, the Tanzania national e-health strategy considers e-healthcare as a "cost-effective" and secure use of information and communication technologies in support of health and its related fields (MoHSW, 2013c). Section 2.4 discusses the status of e-healthcare implementations in the country.

2.4 E-healthcare in Tanzania

E-healthcare is a field at the intersection of medical informatics, public health and business (Eysenbach, 2001). It refers to health care services and resources delivered through information and communication technologies that provides an opportunity for healthcare providers to improve quality of services delivered to patients. E-healthcare also improves patient safety and helps the general public to avoid unnecessary costs. The common information systems that are readily available in the modern healthcare environment include Hospital Information Systems (HIS), Radiology Information Systems, Laboratory Information Systems, Pharmacy Information Systems and Electronic Health Record (EHR) Systems (National Center for Biotechnology Information, 2012). Among these, EHR systems play a significant role in the provision of healthcare services as they store patients' previous medical records and make them available to healthcare professionals and other information systems whenever the need arises.

Currently, hospitals in different ownership groups such as those owned by the government and non-government organisations (including private organisations, parastatal and religious institutions) in Tanzania are implementing electronic healthcare information systems, and in particular EHR systems, as summarised in Table 2.14. As part of this research, a survey was conducted to identify electronic medical or health record systems that have been implemented within the Tanzania healthcare system, together with their respective access control mechanisms (see Appendix B). One notable thing that was identified while conducting this investigation was that, there was neither a national policy nor a legislation designed to protect electronic records from unauthorised access and use which is currently in action in Tanzania. From a close follow-up with the Ministry of Health and Social Welfare (MoHSW) and the newly established, electronic Government Agency (eGA), the researcher was informally notified that there are ongoing efforts aiming to establish a national policy and

a legislation known as Data Protection and Piracy Act. This act is expected to be part of cyber-crime laws, and incorporates access procedures to electronic healthcare records.

Table 2.14: Electronic healthcare information systems implemented in various health facilities in Tanzania

Hospital Name	**System Name**	**Access Control Mechanism**
MNH	Napier-EHR	RBAC
Tumbi Special Hospital	OpenMRS	RBAC
Amana Hospital	–	RBAC
Morogoro Regional Hospital	OpenMRS	RBAC
Ocean Road Cancer Institute	OpenMRS	RBAC
Hindu-Mandal Hospital	Computed Radiography	–
Bugando Hospital	–	RBAC
Mtoni Health Centre	Care2X	RBAC
Haydom Lutheran Hospital	Care2X	RBAC
St. Elizabeth Hospital	Care2X	RBAC
KCMC	Care2X	RBAC
Marangu Lutheran Hospital	Care2X	RBAC
Arusha Lutheran Medical Centre	Care2X	RBAC
Wasso Designated District Hospital	Care2X	RBAC
Tumaini Health Centre	Care2X	RBAC
Kijenge Health Centre	Care2X	RBAC
USA River Health Centre	Care2X	RBAC
Njiro Health Centre	Care2X	RBAC

– indicated as available by the respondent but was not specified

The MoHSW also incorporates several components of healthcare information systems in its current (provisional) national health policy. The Health Management Information System (HMIS), District Health Information System (DHIS), Mobile Health (mHealth) and Short Message Service (SMS) for Life are among the components incorporated for efficient data collection, processing and use. The HMIS was established for the first time in 1994, and aimed at supplying each level of the healthcare sector with necessary information in a timely and accurate manner. The DHIS was aimed to supply each district with necessary data in a timely and accurate manner. The only major difference between HMIS and DHIS lies on size and coverage of the system. While HMIS collects health information from more than 5,400 health facilities, DHIS collects the same information in a smaller capacity. However, despite government efforts to integrate HMIS at the national level, the system has not yet made radical impacts to the healthcare delivery. As pointed out by Smith *et al.* (2008), HMIS focus on managerial activities has been the reason behind its failure.

While mHealth involves the usage of mobile communications technologies, like mobile phones, Personal Digital Assistants (PDAs) and patient monitoring devices, to improve healthcare services and information, SMS for Life aims to help districts to improve stock managements for anti-malaria drugs. As a result of the construction of the National ICT Broadband Backbone (NICTBB) infrastructure and an extensive use of mobile broadband, the implementation of some of these projects is already ongoing. In relation to the overall progress of e-healthcare systems implementation in Tanzania, it is safe to say that the country is still in its infancy stage. Using the Health Information Management Systems Society (H*i*MSS) Care Continuity Model, presented in Table 2.15, Tanzania qualifies to be in either Stage 1 or Stage 2, which is in fact, an infancy stage when it comes to e-healthcare implementation.

Table 2.15: Continuity of Care Maturity Model (Source: HiMSS, 2014)

STAGE	CAPABILITIES
STAGE 7	Knowledge Driven Engagement for a Dynamic, Multi-vendor, Multi-organisational Interconnected Healthcare Delivery Model
STAGE 6	Closed Loop Care Coordination Across Care Team Members
STAGE 5	Community Wide Patient Record using Applied Information with Patient Engagement Focus
STAGE 4	Care Coordination based on Actionable Data using a Semantic Interoperable Patient record
STAGE 3	Normalised Patient Record with Share Care Plans using Structural Interoperability
STAGE 2	Patient Centred Clinical Data using Basic System-to-System Exchange
STAGE 1	Basic Peer-to-Peer Data Exchange
STAGE 0	Limited to No E-Communication

2.5 Conclusions

This chapter provides a background on the Tanzania healthcare system, where both traditional paper-based and electronic health systems are working. The chapter began with a discussion of the healthcare delivery system using a referral pyramid structure, that begins at the community level with the village health services and goes up to treatments abroad. Other units forming the pyramid in a Tanzania healthcare system as shown in Figure 2.2 include regional hospitals serving each region in the country, district hospitals for each district in a region, health centres for divisions and dispensaries. One major observation as a result of an observation survey conducted Muhimbili National Hospital is that, there is a difference between what is written

in official documents as to how health care services should be delivered, and how it operates in the real world. It was clear that the majority of Tanzanians do not follow the referral pyramid structure of the healthcare system and hence, patients make it a habit which is motivated by the availability of better services to pay a first visit to either a district or regional hospitals without being referred by a lower level healthcare facility.

The chapter also discusses characteristics of human resources for health in a Tanzania healthcare system that affect the continuity of care to patients. Among other issues discussed that magnifies the shortage of health workers include, migration of health workers both within the healthcare system and across borders. Since the introduction of horizontal health programmes, health workers are moving from general health services to horizontal health programmes (for better payments) and across borders (for greener pastures), poor governance and an overall lack of investment in human resources, poor living and working conditions and death and retirement. There is also an uneven distribution of healthcare workers in the country (as majority of them are concentrated in urban areas) together with a large number of patients seeking treatments.

To overcome the shortage of health workers in Tanzania while at the same time supporting the continuity of care, it is common to find mid-level healthcare professionals performing basic jobs that were meant for skilled health workers. This thesis, henceforth, supports an existing approach to health care service delivery by proposing a new context-based access control model that allows health workers bypass access rules in case of infrequent emergency access request. This is achieved by extending the traditional Role-Based Access Control (RBAC) model with contexts and obligations. Chapter 3 discusses different mechanisms that are used to control access to protected medical information.

Chapter 3

Access Control

This chapter discusses access control models that have been designed for traditional computing environments. The models discussed include Discretionary Access Control, Mandatory Access Control, Role-Based Access Control and Attribute-Based Access Control. As an example of Discretionary Access Control, an Access Control Matrix has been discussed. The chapter also discusses three implementations of Access Control Matrix, these are: Access Control List, Capabilities List and Authorisation Table. Mainly, this chapter focuses on a discussion of Role Based Access Control, a model which is widely used in healthcare systems today. The rest of this chapter contains the following. Section 3.1 introduces the chapter followed by definitions of terms and concepts in Section 3.2. Section 3.3 reviews traditional access control policies followed by an analysis of their suitability for the healthcare domain in Section 3.4. A new taxonomy for classifying access control models is in Section 3.5. Section 3.6 concludes the chapter.

3.1 Introduction

Access control is used to determine allowed activities of legitimate users, mediating every attempt of a user to access a resource in a system (Ferraiolo *et al.*, 2003), (Hu *et al.*, 2006). Commonly, access control evaluates requests to access resources by already authenticated users, and then it determines whether those requests are granted or denied based on access control policy. In this way access control seeks to prevent activity that could lead to a breach of security (Sandhu & Samarati, 1994).

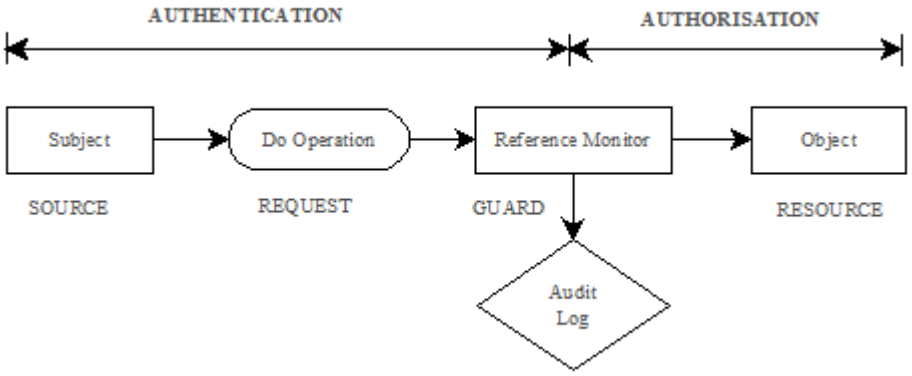


Figure 3.1: Access Control Model (Source: Lampson, 2004)

An access control consists of two major parts, namely, an access control policy and a reference monitor (Krautsevich *et al.*, 2012). Given an access request, an access control policy determines which access requests should be allowed and which ones should be denied. As shown in Figure 3.1, a reference monitor determines whether such an access is authorised or not, by matching an access request against an access control policy. Access control also possesses four general functions: identity verification, authentication, authorisation and auditing, as shown in Figure 3.2. Normally, authorisation to a system is performed after an individual user has been identified and authenticated using for example username and its corresponding password or even using biometrics such as face and hand. After a successful login procedure, cre-

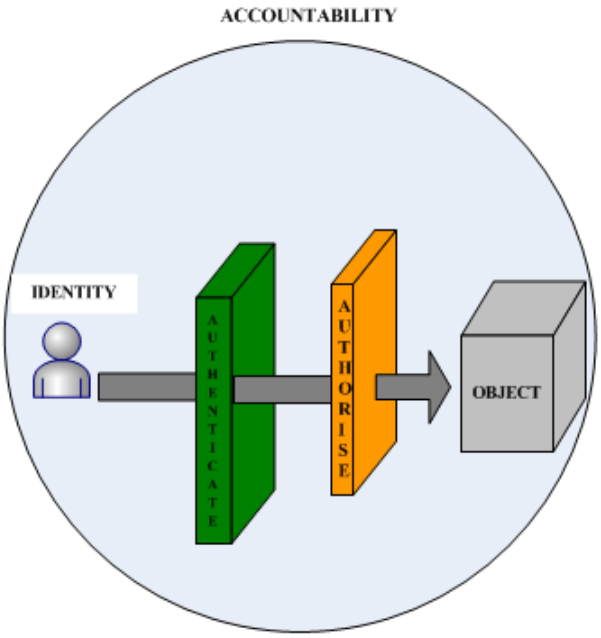


Figure 3.2: Identification, Authentication, Authorisation and Accountability (Source: InfoSec, 2014)

dentials used by an authentication service are then associated with every process an individual user starts.While authorisation tries to answer the question "who is trusted to perform which operations on this object?", auditing gathers decisions made by a reference monitor (including all user access requests and activities). The information collected can then be analysed to discover what happened to the resource and why (Sandhu & Samarati, 1996). In other words, auditing is essential if you need to hold users accountable for their actions. As pointed out by Lampson (2004), authentication, authorisation and auditing altogether form the gold standard for security.

A given Information Technology (IT) infrastructure can implement access control systems in many places and at different levels. Operating systems, for example, use access control to protect files and directories while Database Management Systems (DBMS) apply access control to regulate access to tables and views. Before delving further into a discussion of access control models and their implementations, Section

3.2 defines fundamental elements of an access control policy, that are enforced by an access control mechanism. These concepts, terms and definitions have been referred throughout this thesis.

3.2 Terms and Concepts

This section presents concepts, terms and basic definitions that are commonly used in the access control community, as thoroughly discussed by Hu *et al.* (2006) and Hu & Scarfone (2012):

- **Subject:** is an active entity, generally in the form of a person, process or device, that causes information to flow among objects or changes the system state.
- **Object:** is a passive entity that contains or receives information. It represents a target protected by an access control system. Abstractly, access to an object implies access to the information it contains. Examples of objects are records, pages, blocks, segments, files, directories, directory trees, processes and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, printers, clocks, and network nodes.
- **Operation** is an active process invoked by a subject. When a user of an Automatic Teller Machine enters a bank card and a correct Personal Identification Number, a control program that operates on the user's behalf then allows a subject to initiate one or more operations such as deposit, withdraw and balance inquiry.
- **Permission (or privilege)** is an authorisation to perform some action on a system. A permission corresponds to a privilege a subject owns over a certain object. In most computer security literature, the term permission refers to a combination of object and operation. That being said, when a particular

operation is used on two different objects, it means these are two different permissions. Similarly, two different operations applied to a single object represent two distinct permissions.

As an example of permissions in a banking system, a bank teller may have permissions to execute debit and credit operations on customer records through transactions while an accountant may execute credit and debit operations on the general ledger. With this capability in mind, permissions or privileges can therefore be argued to reduce an access space from where any authenticated subject can access all information to a space where specific users can only perform specific actions on specific objects.

In addition to these terms and concepts which are regarded as the fundamental elements of an access control policy, there are three main abstractions which need to be considered when planning an access control system. These include: an access control policy, access control model and access control mechanism.

- **Access Control Policy:** An access control policy defines high-level security rules that specify how access is managed in a system and who, under what circumstances, may access what information. They can either be application specific, and hence be taken into account by an application vendor, or only applicable to user actions within an organisation unit or across organisational boundaries. Access control policies may also pertain to object usage within or across organisational units, need-to-know, competence, authority and obligation. Usually, the suitability of a given access control policy depends on protection requirements for a given system, environment and users.

- **Access Control Model:** This is a formal representation of a security policy enforced by an access control that presents limitations of a system. An access control model can either be defined as a formalised computing algorithm,

mathematical representation or a well-recognised formal concept. Roles, Multi Level Security (MLS) and Usage Control are formal concepts used in Role-Based Access Control, Mandatory Access Control and Usage Control models respectively. Since access control models bridge a wide gap in abstraction that exists between access control policies and mechanisms, they are of general interest to both users and application vendors. Abstractly, an access control mechanism can be designed to adhere to the properties of a model.

- **Access Control Mechanism:** At a high level, an access control policy is enforced through an access control mechanism that translates user's access request in terms of a structure that a system provides. An access control mechanism defines low level (both hardware and software) functions that implement control imposed by an access control policy and formally stated by the model in order to prevent unauthorised access to resources. The majority of traditional access control mechanisms are based on the notion of a reference monitor that authorises access to resources managed by the system. The actions are either permitted or denied based on the privileges established in the system and expressed in terms of access rights (Sandhu & Samarati, 1994).

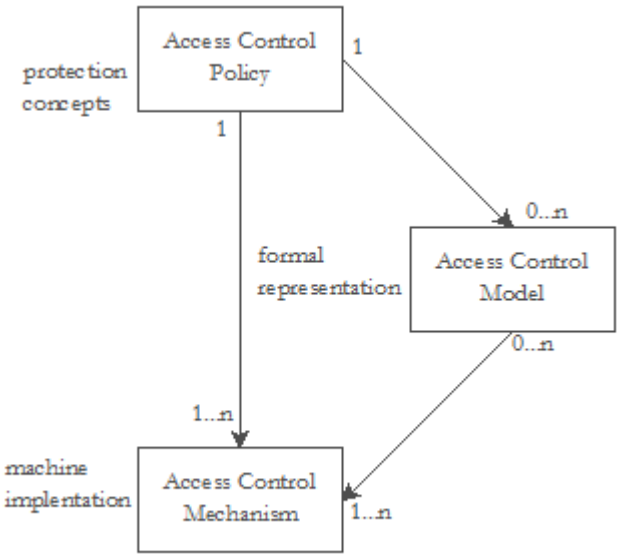


Figure 3.3: Mappings of an access control policy, model and mechanism (Source: Hu & Scarfone, 2012)

The relations and mappings between the access control policy, model and mechanism is presented in Figure 3.3. An access control system is actually initiated by an access control policy, which is then formalised by an access control model, if there is any that can be applied. An access control policy is physically implemented by software or hardware mechanisms based on an access control policy directly or by an access control model, indirectly. All the mapping relations between the access control policy and model, the access control policy and mechanism and the access control model and mechanism are one-to-many. Section 3.3 reviews common access control policies.

3.3 Access Control Policies

This section discusses three major access control policies that have emerged since 1970s: Discretionary Access Control, Mandatory Access Control and Role-Based Access Control. This section also reviews a successor of Role-Based Access Control called

Attribute-Based Access Control.

3.3.1 Discretionary Access Control

The Trusted Computer Security Evaluation Criteria (TCSEC)(1985) defines DAC as "a means of restricting access to objects based on the identity of subjects and/or groups to which they belong". The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject unless restrained by Mandatory Access Control (Ferraiolo *et al.*, 2003), (Hu *et al.*, 2006). In other words, DAC allows an owner of a particular access right to a specific object to pass on access right to other subject(s) based on the owner's personal preferences. This capability makes the DAC model more flexible in supporting commercial solutions where no strict information flow is required.

The manipulation of a shared folder on a server is one sample application that can benefit from this capability of DAC. The owner (let's say Anne) with an access right "read" over a shared folder can easily pass this access right to another subject (Alice, for example) by creating a username and password pair associated with Alice. Since Anne can pass her read access right to any subject at her discretion and the system manager is unable to control any of this from happening, there is, in fact, no real control on flow of information provided by the mechanism. This lack of information flow control increases the possibility of unauthorised access and thus, the approach is not considered suitable for military applications which require a rigorous control of information flow (Biba, 1977), (Proctor & Wong, 1989), (Sandhu & Samarati, 1994).

Access Control Matrix (ACM) is one of the first discretionary access control models for computer systems. As defined by Sandhu & Samarati (1994), ACM is a conceptual model that specifies access rights each subject possess for each object that is managed

by the system. This classic model was first proposed by Lampson (1971) for protection of resources within an operating system and later refined by Graham & Denning (1972). The model was then formalised by Harrison *et al.* (1976) and called the Harrison, Ruzzo and Ullman (HRU) security model. More specifically, Harrison *et al.* (1976) developed an access model proposed by Lampson (1971) to a goal of analysing the complexity of determining the access control policy. The HRU formalisation identified six primitive operations which had an impact on the authorisation state of ACM. These are: adding and removing subject, adding and removing an object and granting and revoking a privilege.

The original model was referred to as an access matrix because an authorisation state is presented as a matrix that contains a row for each subject and a column for each object. Each cell of a matrix denotes an access authorised for a subject in a row to an object in a column. The main function of an access control system with an ACM approach is to ensure that only operations authorised by the matrix are executed on objects. This is achieved by the means of a reference monitor, responsible for assuring that all operations are of the right kind and all attempted operations by the subject on object are authorised (Anderson, 1972), (Sandhu & Samarati, 1994), (Samarati & de Vimercati, 2001).

In addition to its ability to implement security policies in ACM, other objectives of a reference monitor, as discussed by Anderson (1972), are:

- Tamper proof: This means a reference monitor cannot be changed either programatically (by malicious code) or manually to guarantee its integrity.
- Invoked: The continuous invocation of a reference monitor means a subject cannot avoid access control even if it is an operating system itself.
- Verifiable: This means a reference monitor is correct and an implementation of

a security policy can be logically demonstrated.

Conceptually, an access control mechanism implementing the ACM policy should be able to answer the question "does subject (S) has right (R) for object (O)?". This question can be represented as a triple (S, O, A) where S represents a set of subjects wishing to exercise privileges, O is a set of objects on which privileges can be exercised and A is a matrix with rows representing subjects and columns representing objects. The model includes the access checking rule $A[s, o]$ which ensures that an access request to an object o is denied if $A[s, o]$ does not contain an access right. The model also contains a set of commands specifying how to make transitions in (S, O, A).

$$A = A[s, o] s \in S, o \in O, A[s, o] \subseteq A \tag{3.1}$$

Mathematically, the access matrix (A) can be defined using equation 3.1 where access $A[s, o] \subseteq A$ represents operations that subject $s \in S$ can perform on object $o \in O$ and A denotes a set of all access operations that a subject can perform on an object.

Table 3.1: Access Control Matrix (Source: Sandhu & Samarati (1996))

	File 1	**File 2**	**File 3**	**File 4**
Anne	OWN R W	-	OWN R W	-
Bob	R	OWN R W	R W	R
Alice	R W	R	-	OWN R W

A simple example of the ACM model is presented in Table 3.1, where OWN, R and W denote Owner of the file, Read and Write access rights respectively. From this matrix, a system is keeping track of four files: File 1, File 2, File 3 and File 4 that can be

accessed by three subjects: Anne, Bob and Alice. The matrix specifies a relationship between subjects and the four files as follows: Anne is the owner of File 1 and File 3 and can Read and Write in those files. Anne has, however, no access to File 2 and File 4. Bob is the owner of File 2, can read File 1 and File 4, and can read and write in File 3. Alice owns File 4 and can read and write in that file. She can also read and write in File 1, read only in File 2, and she has no access at all to File 3.

There are various approaches for implementing access matrix in practical large systems. The well-known ones include Access Control List (ACL), Capability List (CL) and Authorisation Table (AT).

Access Control List

Access Control List (ACL) is, perhaps, the most popular approach for implementing Access Control Matrix (ACM) in practical systems. ACL is a list of permissions attached to an object, such that each object is associated with an ACL. It is also regarded as storing ACM in a columnar way. It specifies which users or system processes are granted access to objects and what operations are allowed on given objects. This means that, for each subject using a system, there is a list of access rights such a subject is allowed to execute on an object, thus, each entry in a list is a pair of subjects and a set of access rights. As summarised by Samarati & de Vimercati (2001) and depicted in Figure 3.4, ACL implementations are object-centric because they specify an object's legitimate access modes.

By examining an object's ACL, it is straight forward to determine which modes of access a subject is currently authorised for an object. It is also easy to revoke all accesses defined for an object by replacing existing ACL with an empty one (Samarati & de Vimercati, 2001). However, despite its simplicity, determining access rights of a subject is not easy and revocation of subject's accesses is tedious as it re-

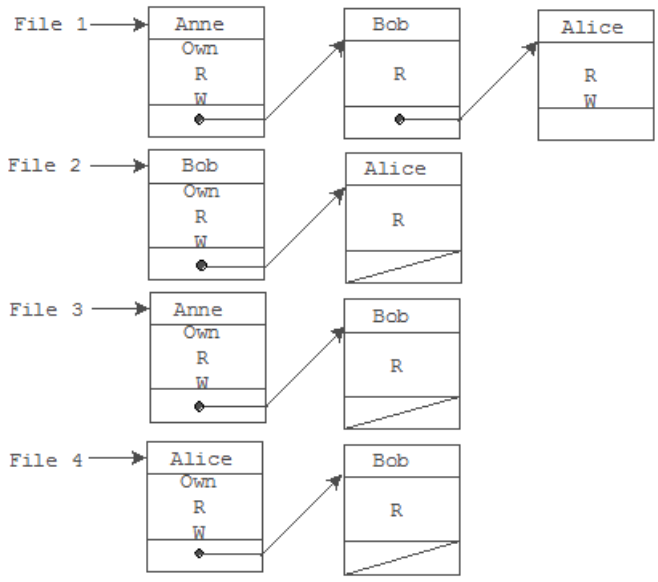


Figure 3.4: Access Control List (Adapted from: Sandhu & Samarati, 1994)

quires every ACL in the system to be checked against a subject (Samarati & de Vimercati, 2001).

Capability List

Capability List (CL) is another implementation of the ACM. Unlike ACL approach which stores ACM in columns, CL stores it in rows. Each subject in a system is associated with a capability created from the corresponding row of an access matrix, indicating access rights each subject is authorised to execute on an object. The capabilities in ACL are subject-centric, as depicted in Figure 3.5. This actually solves the problem of determining a set of allowed actions by a specific subject by just examining the subject's associated capabilities. However, revoking an object's access mode in CL requires an examination of each and every subject's capability list.

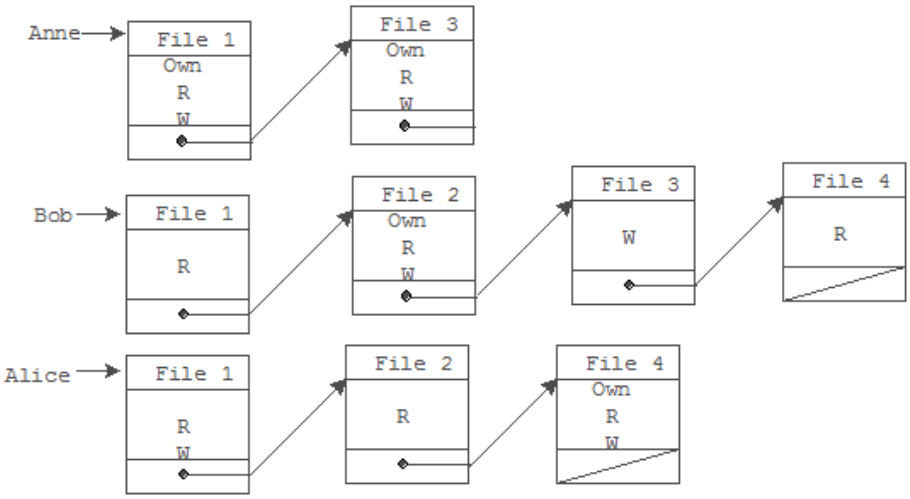


Figure 3.5: Capability List (Adapted from: Sandhu & Samarati, 1994)

Authorisation Table

Authorisation Table (AT) is another implementation of Access Control Matrix (ACM) inspired by the relational databases. Non-empty entries in a relational table are presented with three columns: Subjects, Actions and Objects. Each row represents an access operation a subject can perform on a specific object. This implementation does not favour one preview over the other, as ACL and CL do. It is also easy to get specific subject's access rights by sorting the table by either a subject, which actually corresponds to CL method, or by object, which produces the same effect as ACL. Table 3.2 presents an example of an authorisation table. In the first row of the authorisation table, it shows that Anne is an owner of File 1.

DAC Summary Remarks

It is worth noting that managing ACM in a large-scale distributed environment is troublesome. First and foremost, ACM is a static access control solution where subjects and objects need to be predefined. In a large-scale distributed environment with

Table 3.2: Authorisation Table (Adapted from: Sandhu & Samarati, 1994)

User	Access Mode	Object
Anne	OWN	File 1
Anne	Read	File 1
Anne	Write	File 1
Anne	OWN	File 3
Bob	Read	File 1
Bob	OWN	File 2
Bob	Read	File 2
Alice	Read	File 1
Alice	Write	File 1
Alice	Read	File 2
Alice	OWN	File 4

hundreds of users and thousands of files, the approach becomes costly in terms of storage and space. ACM also becomes inappropriate since the matrix becomes sparse and most of the cells are likely to be filled with zeros (Samarati & de Vimercati, 2001), (Zhang *et al.*, 2005b). It is also not easy to impose constraints in DAC, thus, the approach is considered not to be suitable for the dynamic and collaborative environments like healthcare. The Discretionary Access Control (DAC) also results into information leakage caused by weak control of information flow. To solve the problem of information leakage within DAC models, Mandatory Access Control was established with unbreakable rules that are designed to ensure respect for access control demands. The Mandatory Access Control model, discussed in detail in Section 3.3.2, gives subjects and objects several levels that cannot be changed by the user, and consequently limits their power to manage access to their data.

3.3.2 Mandatory Access Control

The key motivation behind Mandatory Access Control (MAC), first formalised by Bell & LaPadula (1973), was to overcome the problem of malicious and flawed software faced by DAC approaches. Its goal was to achieve mandatory access control so that access decisions will not be left at the discretion of an individual user or a system administrator, but rather through an organisation's security levels (Sandhu, 1993). TCSEC (1985) defines MAC as a "means of restricting access to objects based on the sensitivity contained in an object (represented by a security label) and the formal authorisation (that is, clearance) of subjects to access information of such sensitivity". Unlike DAC where access rights are defined by the resource owner based on the resource owner's discretion, MAC enables access rights to be determined by a manager or a central authority of the system, and users do not have an ability to override an access policy.

$$ts > s > c > u \tag{3.2}$$

MAC policy is widely used in military and civilian governments, and is expressed in terms of a security label attached to both objects and subjects (Sandhu, 1993). A label attached to an object, which reflects the sensitivity of information, is called a "security classification" and a label attached to a subject reflects the user's trustworthiness not to disclose sensitive information and is called a "security clearance". The assignment of access rights is performed by a central authority not by the resource owner. Access to a resource object is restricted to those subjects who possess a valid clearance level (also known as authorisation). A simple form of MAC is represented mathematically using Equation 3.2, and also shown in Figure 3.6 where hierarchical set of security levels consists of top secret (ts), secret (s), confidential (c) and unclassified (u).

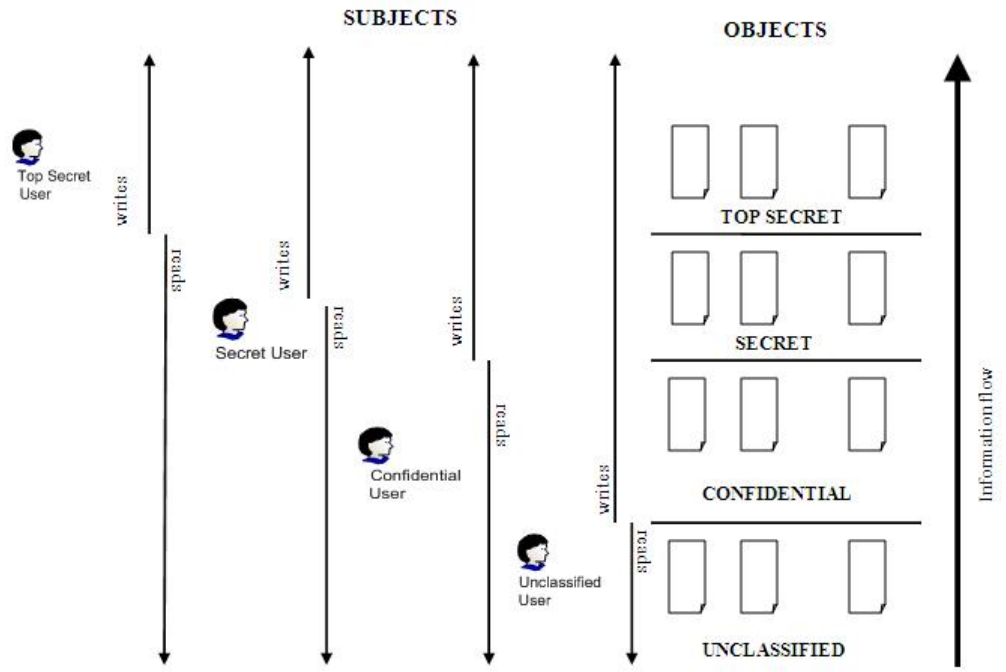


Figure 3.6: Controlling information flow for secrecy (Source: Sandhu & Samarati, 1994)

The flow of information dissemination in one direction (either from low to high confidentiality or equivalently, from low to high integrity) is one among the strongest features of MAC. Despite such a capability that reduces the likelihood of potential illegitimate information leakage, MAC model is vulnerable to covert channel attacks (Sandhu, 1996a). As defined by Lampson (1973), covert channels are "those channels not intended for information transfer at all, such as the service program's effect on system load". The channels can, however, be abused to allow information to be communicated between parties, which are not supposed to do so. The idea of the attack is centred on adding capabilities between entities to illicitly transfer information, thus, breaking the security policy of the system. In other words, it is a kind of collusion between the sender and the receiver in a clear violation of the MAC security policy. These attacks are expensive to eliminate even if they are identified and analysed (Sandhu, 1996a).

MAC Summary Remarks

It is useful to note that the MAC model suits access control requirements where an object's access right is determined by a central authority and not at the discretion of the object owner (Sandhu & Samarati, 1994), (Ferraiolo *et al.*, 2003). In addition to its capability to resolve the problem of information leakage that the DAC model experiences, MAC remains to be a very rigid model for commercial domains. It does not allow the user to manage exceptions between different security levels. This feature of the MAC models results in the overall approach being characterised as static, which makes it inappropriate for the dynamic and collaborative environments such as healthcare that require dynamic context information to support the continuity of care (McCollum *et al.*, 1990).

3.3.3 Role-Based Access Control

Role-Based Access Control (RBAC) is an access control model that governs access to resources based on a subject's organisational role. As defined by Hansen & Oleshchuk (2003), a role is a "collection of permissions on a set of objects, which are determined by the system, based on user's enterprise activities, responsibilities and policies of the organisation". The central notion behind RBAC is that permissions are administratively associated with roles and users are made members of appropriate roles, and thus acquiring role permissions (Ferraiolo *et al.*, 1995). In an organisation that adopts RBAC, roles are usually created based on job functions and users are assigned roles based on their responsibilities and qualifications. Such a natural mapping between roles and an organisational structure makes it easy to assign and reassign users from one role to another. Roles can also be granted new permissions as new applications are incorporated and permissions can be revoked from roles as needed. The relationship between users, roles and permissions is many-to-many (using double arrows), as

shown in Figure 3.7. Each user can be associated with one or more roles and each role can have one or more permissions associated with it.

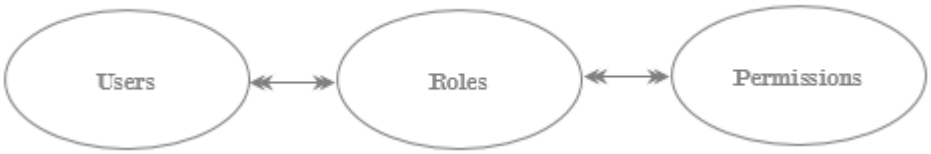


Figure 3.7: Users, Roles and Permissions

Constraints can be imposed on access requests to prevent unauthorised access or malicious activities in role based systems. Among the supported constraints are: a "least privilege" principle, in which no user should be given more privilege than necessary to finish the task at hand (Sandhu & Samarati, 1994). In this way RBAC prevents the leakage of access rights to unauthorised entities and also reduces the risk of fraud. The model also supports the separation of duty constraints which places a restrictive rule on the potential inheritance of permissions from opposing roles. As an example of separation of duty, a single person in a banking organisation should not be allowed to perform both "authorise creation of an account" and "creation of banking accounts". Additionally, RBAC allows organisations to separate superuser capabilities from normal users and assign them to special user accounts, through its support for role hierarchies.

Historically, the first RBAC model known as RBAC92 was proposed by David & Richard (1992) in 1992 by identifying and defining concepts related to the concept of roles. The RBAC92 model was subsequently extended by Sandhu *et al.* (1996) in order to propose a conceptual framework that can be used as a basis for implementing RBAC based solutions. As a result, RBAC96 model was introduced. In the years that followed, RBAC became a predominant model for advanced access control due to its high

performance that reduces cost of deployment and maintenance. This motivated the National Institute of Standards and Technology (NIST) to call for a unified standard by integrating RBAC92 and RBAC96 in the year 2000. Since the research carried out in this thesis is based on RBAC model, an overview RBAC96 and the resultant NIST RBAC model are provided. The review focuses on their organisation levels as well as formal definition of their core models.

RBAC96 Model

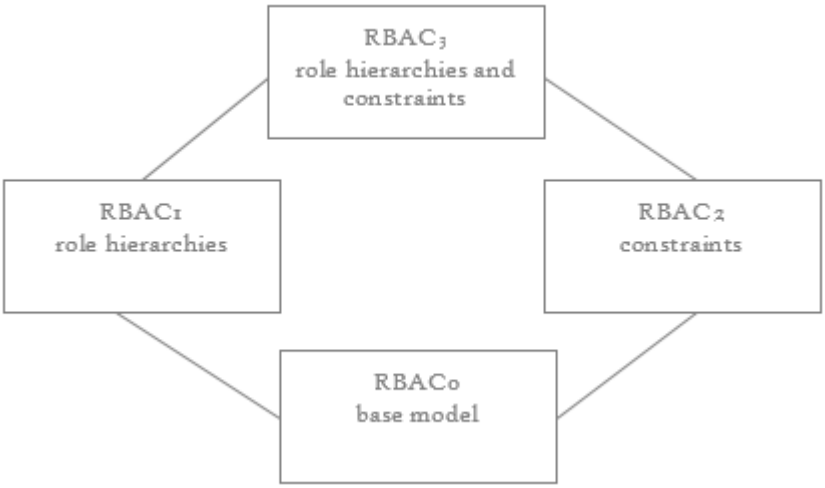


Figure 3.8: RBAC96 Family of Reference Models (Source: Sandhu *et al.*, 1996)

Sandhu *et al.* (1996) proposed a family of four conceptual RBAC models, as summarised in Figure 3.8. The model comprises of $RBAC_0$ (a base model, indicating that it is the minimum requirement for RBAC implementations), $RBAC_1$ (comprising of $RBAC_0$ with a support of role hierarchies), $RBAC_2$ (includes $RBAC_0$ with support of constraints that impose restrictions on acceptable configurations on different components of RBAC). Also, there is $RBAC_3$, known as a consolidated model, which includes $RBAC_1$ and $RBAC_2$, and by transitivity $RBAC_0$.

The core RBAC96 model consists of five sets of entities, including Users (U), Roles (R),

Permissions (P), Administrative Roles (AR) and Administrative Permissions (AP). Intuitively, a user is a human being or any other autonomous intelligent agent like a robot or immobile computer. A role is a job function or job title within an organisation that indicates authority and responsibility conferred on a member of a role. Permissions refer to an approval of a particular mode of access to one or more objects in a system (Sandhu *et al.*, 1996) .

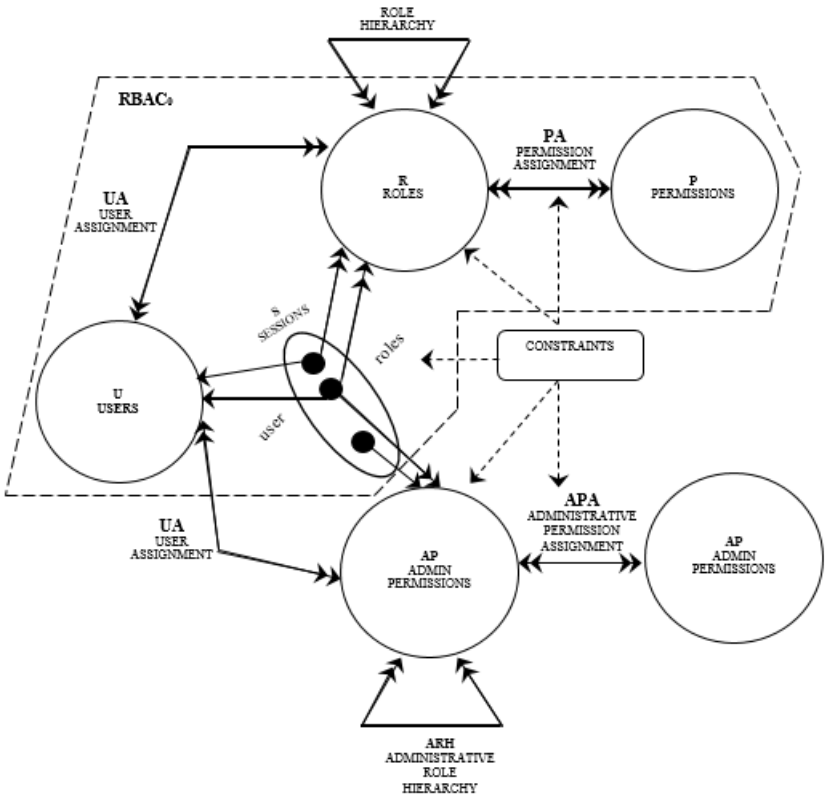


Figure 3.9: The RBAC96 Model (Source: Sandhu *et al.*, 1996)

Unlike Discretionary Access Control (DAC) which allows both positive (which means, give access) and negative permissions (deny access), RBAC96 model allows only positive permissions which confer to an ability of a permission holder to perform one or more actions in system objects. Additionally, Administrative Permissions (AP) control operations which modify components of RBAC, such as adding new users and

roles or modifying user assignment and permission assignment relations. The APs can only be assigned to Administrative Roles (ARs).

Mathematically, RBAC96's core model (RBAC_0) by Sandhu *et al.* (1996) can be represented as follows:

Definition

- U is a set of Users
- R is a set of Roles
- P is a set of Permissions
- $UA \subseteq U \times R$, a *many-to-many* user-to-role assignment relation.
- $PA \subseteq P \times R$, is a *many-to-many* permission-to-role assignment relation.
- S is a set of Sessions.
- $user : S \rightarrow U$, is a function mapping each session s_i to the single user $user(s_i)$, and is constant for the session's lifetime.
- $role : S \rightarrow 2^R$ is a function mapping each session s_i to a set of roles, $\text{roles}(s_i) \subseteq \{r|((\exists r' \geq r)[(user(s_i, r') \in UA\}$ (which can change with time) and session s_i has the permission $U_{r \in role(s_i)}\{P|(\exists r'' \leq r)[(p, r'') \in PA\}$
- There is a collection of constraints stipulating which values of different components of RBAC model are allowed or forbidden.

NIST RBAC Model

According to Sandhu *et al.* (2000), the basic concept of the RBAC model is that users are assigned to roles through "user assignment" relation and permissions are assigned to roles through "permission assignment" relation. Particularly, user assignment defines a set of roles to which an individual user can be mapped. For example, user (named Anne) could be assigned to a role set {*Doctor, Emergency Doctor, Specialist Doctor*}. In fact, user assignment determines the super set of roles to which user can be mapped as part of the user's organisational duties. Permission Assignment, on the other hand, specifies a set of allowed activities for a given role. It corresponds to assigning access rights to roles. The emergency doctor role, for instance, could claim

the following access rights {*write to the patient's EHR, read patient's EHR, read past medical history of a patient*}.

The RBAC model requires that user assignment and permission assignment relations to be many-to-many whereas each user can be assigned to many roles and each role can have many users. Also, there is a many-to-many relation between roles and permission. As such, each role can be assigned to many permissions and each permission can be assigned to many roles. Users acquire permissions by being members of defined roles.

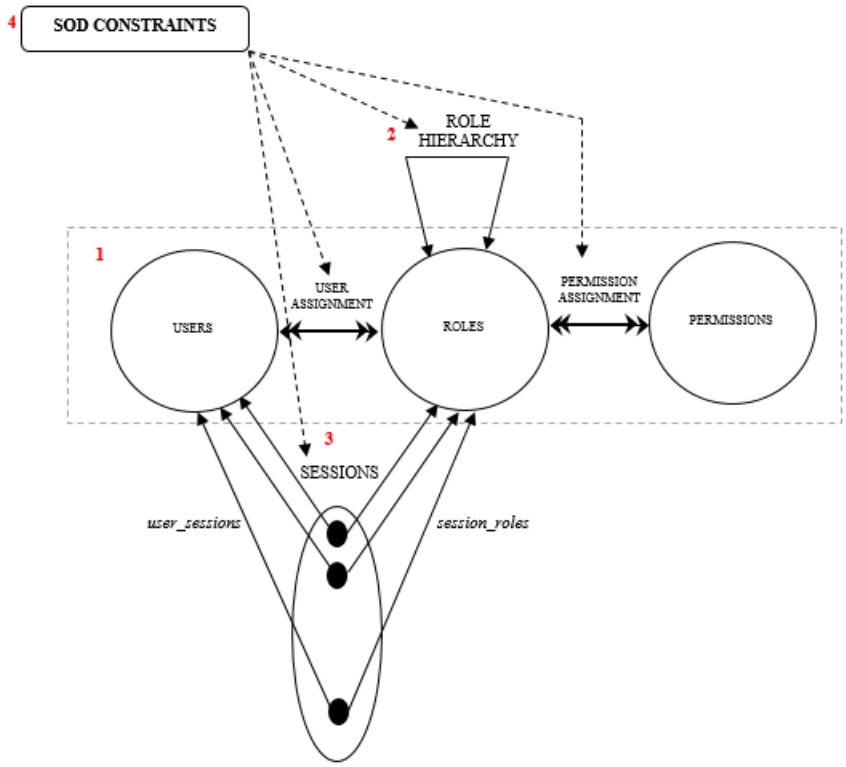


Figure 3.10: NIST RBAC capabilities (Source: Sandhu *et al.*, 2000)

Similar to RBAC96, the NIST RBAC model is organised into four levels with increasing functional capabilities (Sandhu *et al.*, 2000). As presented in Figure 3.10 (labelled number 1 to 4) and its functional capabilities summarised in Table 3.3, the four levels of NIST RBAC model are:

i. Core RBAC, also known as Flat RBAC

ii. Hierarchical RBAC

iii. Constrained RBAC and

iv. Symmetric RBAC

Table 3.3: Variations of NIST RBAC model organised as levels
(Source: Sandhu *et al.*, 2000)

Level	**Name**	**RBAC Functional Capabilities**
1	Flat RBAC	– users acquire permissions through roles – must support many-to-many user-role assignment – support many-to-many permission role assignment – must support user-role assignment review – users can use permissions of multiple roles simultaneously
2	Hierarchical RBAC	Flat RBAC and – must support role hierarchy (partial order) – level 2a requires support for arbitrary hierarchies – level 2b denotes support for limited hierarchies
3	Constrained RBAC	Hierarchical RBAC and – must enforce Separation of Duties (SOD) – level 3a requires support for arbitrary hierarchies – level 3b denotes support for limited hierarchies
4	Symmetric RBAC	Constrained RBAC and – must support permission-role review with performance effectively comparable to user-role review – level 4a requires support for arbitrary hierarchies – level 4b denotes support for limited hierarchies

The core NIST RBAC model includes five sets of elements. These are: Users, Roles, Objects, Operations and Permissions. Like RBAC96, the NIST RBAC model is defined in terms of individual users being members of roles and permissions being assigned to roles. A role is a way of naming many-to-many relations between users and permissions. An operation is an executable image of a program, upon invocation

executes some function for the user. An object is an entity that contains or receives information. Ferraiolo *et al.* (2001) represent these entities mathematically as follows:

Definition

- USERS, ROLES, OPS and OBS represent users, roles, operations and objects, respectively
- $UA \subseteq USERS \times ROLES$, a *many-to-many* mapping user-to-role assignment relation.
- $assigned\_users : (r : ROLES) \rightarrow 2^{USERS}$, the mapping of role r onto a set of users. Formally: $assigned\_user(r) = \{u \in USERS | (u, r) \in UA\}$
- PRMS $= 2^{(OPS \times OBS)}$, representing a set of permissions
- $PA \subseteq PRMS \times ROLES$, a *many-to-many* mapping permission-to-role assignment relation.
- $assigned\_permissions(r : ROLES) \rightarrow 2^{PRMS}$ mapping of role r onto a set of permissions. Formally: $assigned\_permissions(r) = \{p \in PRMS \ | (p, r) \in PA\}$
- $ob(p : PRMS) \rightarrow \{op \subseteq OPS\}$, the permission-to-operation mapping, which gives the set of objects associated with permission p.
- $ob(p : PRMS) \rightarrow \{ob \subseteq OBS\}$, permission-to-object mapping, which gives the set of operations associated with permission p.
- SESSIONS representing a set of sessions
- $user\_sessions(u : USERS) \rightarrow 2^{SESSIONS}$, mapping of user u onto a set of sessions
- $sessions\_roles(s : SESSIONS) \rightarrow 2^{ROLES}$, mapping of session s onto a set of roles. Formally: $session\_roles(s_i) \subseteq \{r \in ROLES | session\_users(s_i), r) \in UA\}$
- $avail\_session\_perms(s : SESSIONS) \rightarrow 2^{PRMS}$, the permissions available to a user in a session $\bigcup_{r \in session\_roles(s)}$ assigned_permissions(r).

Advantages of RBAC

There are numerous reasons as to why RBAC is regarded as a generalised approach to security management (Hansen & Oleshchuk, 2003), (Joshi *et al.*, 2005). One important characteristic is, by itself RBAC is policy neutral. It actually provides a means of articulating a policy rather than embodying a particular security policy (Sandhu, 1996a). The RBAC enforced in a particular system is, in fact, a result of precise system configuration and interactions between various system components (Osborn *et al.*, 2000).

To demonstrate this capability of RBAC, Sandhu (1996b) shows how traditional lattice-based MAC can be simulated using the RBAC model and Osborn *et al.* (2000) demonstrate how RBAC can be configured to enforce both discretionary and mandatory access control policies. More generally, Sandhu (1996a) and Osborn *et al.* (2000) established that traditional MAC is just one instance of RBAC as a single Trusted Computing Base (TCB) which can be configured to enforce RBAC in general and MAC in particular. RBAC is also credited for its ability to modify security policy to meet the demanding needs of a commercial organisation. Its flexibility has resulted in this generic access control approach being recommended in various legislation such as Health Insurance Portability and Accountability Act (HIPAA) (Franqueira & Wieringa, 2012).

Limitations of RBAC

Despite its benefits and being widely adopted, RBAC has some limitations. Oh & Park (2003) identify two of its limitations. These are:

1. There is no clear separation between two concepts: a "role" and a "task". In a real organisation, a task may sometimes require an involvement of multiple roles.

2. Role inheritance in RBAC does not fully reflect the same process in real organisations. As a concept in RBAC, when role R_1 (a higher role) inherits from another role R_2 (a lower role), this means that R_1 inherits full permissions set of R_2. In a real organisation, however, a higher role only inherits partial permission set of a lower role.

Additionally, access control decisions in modern and collaborative environments like healthcare are dynamic, and as such privileges and capabilities of users tend to change. The access rights in these environments may henceforth not solely depend on indi-

vidual user's identities. They may, however, depend on context in which an access request is made. This may include the user's context, such as location of access and time when an access request was sent, and the system's context which may include system load and network state. The RBAC model is , in fact, not able to consider context information in access control decision making (Kuhn *et al.*, 2010). To enforce dynamic context information using RBAC, particularly in large organisations, a "role explosion" can result in thousands of separate roles being fashioned for different collections of permissions. The fact that access control policies in RBAC are presumably static (that is, they follow the same access control requirements regardless of any change in the surrounding environment), hinders the application of RBAC to achieve a more fine-grained access control required in many modern environments such as in electronic healthcare to support the continuity of care.

3.3.4 Attribute Based Access Control

Attribute-Based Access Control (ABAC), which is sometimes referred to as Policy-Based Access Control (Blaze & Keromytis, 1999), (Pimlott & Kiselyov, 2006) or Claims-Based Access Control (Brown, 2007), has been proposed as a solution to problems identified in RBAC, including role explosion which results from the model's inability to support context information in its access decisions. ABAC is defined as a "new generation" access control model that provides dynamic, context-aware and risk-intelligent access control. This approach is, thus, praised for its ability to achieve efficient regulatory compliance, reduced time-to-market for new applications and a top-down approach to governance through transparency in policy enforcement.

With the help of a structured language like eXtensible Access Control Markup Language (XACML), ABAC uses attributes as building blocks in a structured language that describes access requests and defines access control rules (Karp *et al.*, 2009).

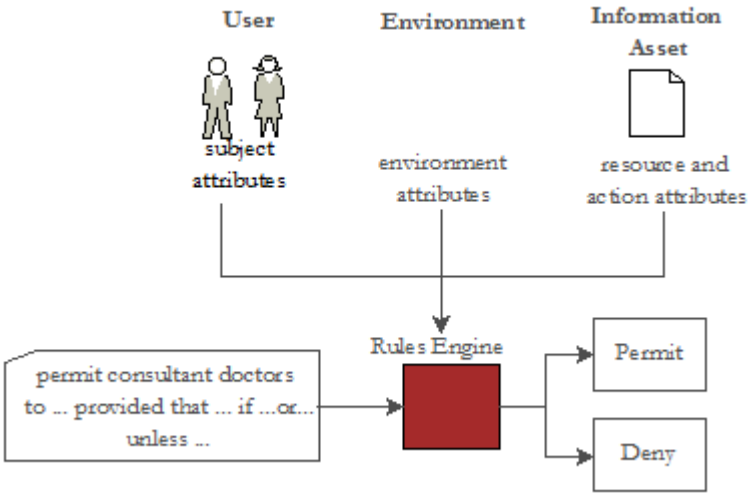


Figure 3.11: Attribute Based Access Control approach

Generally, ABAC specifies a claim or claims that need to be satisfied in order to grant access to a resource, and any user who can prove such a claim is granted access to a resource. For an ABAC policy that contains a claim "above 18"; any person who can prove that he or she is above 18 years old is granted access. The attributes in ABAC are categorised into three groups, these are: Subject, Resource and Environment. A subject is an entity requesting access to perform an action on a resource. Each subject is associated with a number of attributes including user identification, role, group memberships, department or company to which user belongs, competencies and management level.

Other attributes in ABAC are collected from the action the user wants to perform on the object, and a resource which is acted upon by a subject. A Microsoft Word document is an example of a resource, and may contain attributes such as name, title, date and so on. The environment attributes, on the other hand, represent operational, technical and situational attributes that may need to be considered before permitting

```
<Request  xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <Subject>
      <Attribute  AttributeId=
                      "urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                   DataType="http://www.w3.org/2001/XMLSchema#string">
          <AttributeValue>nurse</AttributeValue>
       </Attribute>
   </Subject>
<Resource>
       <Attribute AttributeId=
    "urn:oasis:names:tc:xacml:1.0:resource:resource-id"
     DataType="http://www.w3.org/2001/XMLSchema#string">
      <AttributeValue>localhost:8080/roc-bac-sys</AttributeValue>
   </Attribute>
</Resource>
<Action>
  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:
           action-id" DataType="http://www.w3.org/2001/XMLSchema#string">
         <AttributeValue>read</AttributeValue>
  </Attribute>
</Action>
</Request>
```

Figure 3.12: Access Request in XACML (Source: Author)

or denying access to a resource. They identify context in which access is requested. Common environment attributes include current time and location from where the access request occurred. These attributes can be of any type that is relevant to consider so as to minimize risks or to plan for precautions. An access control request written in XACML is presented in Figure 3.12. The request contains three attributes, these are: subject-id (identifies each subject), resource-id (for an identification of a resource) and action-id (for action's identification). These attributes contain values "nurse", "localhost:8080/roc-bac-sys" and "read" for subject-id, resource-id and action-id attributes respectively. An analysis of the discussed access control policies for a modern healthcare environment is in Section 3.4 and a classifications of access control models is in Section 3.5.

3.4 Access Control Policy for Healthcare

This section analyses the suitability of discussed policies to control access in a modern healthcare environment.

Discretionary Access Control (DAC)

In a modern healthcare environment, DAC can be implemented as follows: "users" of the system may include patients, healthcare professionals and other stakeholders such as insurance companies. While "objects" are fields in a patient's EHR, "operations" consist of actions that individual users can perform to an object.

These may include create, read, update and delete. Although theoretically it seems feasible to implement DAC in a modern healthcare environment, there are, however, some functionality challenges that make it inappropriate (Baker *et al.*, 1997). One common challenge that has been reported in literature is the question of *ownership of EHRs* and who controls their access when a patient dies. In fact, this question which can have layers of complexity seems to be both unanswerable and inadequate for the domain, and thus it has sparked a debate as to who is a true owner of these sensitive medical records. That is, between a patient to whom records are referred, healthcare professionals who create the records, Information Technology (IT) specialist (that is, a system administrator) who maintains the records and has greater control over them, or a healthcare provider or organisation through which medical records are stored in their infrastructure (Trotter, 2012).

Using HIPAA regulation, for instance, to evaluate access rights to EHR for different entities, as illustrated in Table 3.4, neither a patient nor a healthcare provider are regarded as true owners of EHRs. Typically, a "true owner" of any product would be able to destroy and change the products they own without recording what changes

Table 3.4: HIPAAs access rights to EHRs for different entities (Source: Trotter (2012))

Person or Privilege	Delete their copy of data	(Arbitrarily (without logs) edit their copy of data	Correct the Provider's copy of data	Append to the provider's copy of data
Health Provider	**No**. HIPAA does not allow providers to delete copies of patient records	**No**. HIPAA does not allow changes to the contents of EHR without a log of those changes being maintained	**Yes**. Providers can correct their copy of EHR data, providing that they maintain a copy of the incorrect version	**Yes**. Providers can add to EHR data, without changing the "correctness" of the previous instances of the data
Patients	**Yes**. They can delete their own copies of their patient records, but requests to providers that their chart should be deleted will be denied	**No**. Patients cannot change the "canonical" version of patient record	**No**. Patients can only suggest that the "canonical" version of patient record be updated	**Yes**. Under HIPAA, patients has the right to append EHR records
IT Specialist	**Kind of**. Regulations dictate that IT specialists and vendors should not have the right to delete patient records. But, through root or administrative access to the underlying databases this can be achieved	**Yes**. Source code or database-level access ensures that patient records can be modified without logging	**Yes**. Source code or database level access ensures that patient records can be modified without logging	**Yes**. Source code or database level access ensures that patient records can be modified without logging
True Copyright Ownership	**Yes**. You can destroy things you own	**Yes**. You can change things you own without recording what changes you have made	**No**. If you hold copyright to the material and someone has purchased a right to a copy of that material, you cannot make them change it	**No**. You have no rights to change another person's copy of something you own the copyright to

have been made. They would also be held responsible for any unauthorised disclosure of protected information, and be able to control contents of their products. For the healthcare domain, however, this is not the case because if patients are granted full control to their EHRs, this would definitely change the current fundamentals of medical practice.

In addition to true ownership, the usage of DAC in a healthcare sector may result into unscalable permissions. As pointed out by Grimson (2001), EHR is a longitudinal

healthcare record of the patient which spans from cradle-to-grave. From this definition, it means that as the time passes the amount of patient's records increases. And as the number of users and records grow, it becomes difficult to update permissions when using DAC (Pervaiz *et al.*, 2010). Alhaqbani & Fidge (2007) also point out the possibility of creating new security challenges that might be caused by patient mismanagement of their own records when DAC is used in the healthcare sector.

Mandatory Access Control

Conceptually, the implementation of a MAC-based approach in a modern healthcare environment will involve definition of security levels for both subjects and objects. Based on job functions in a healthcare domain, common levels for subjects may include a system administrator, doctor (who can be defined further with different levels such as consultant doctor, specialist doctor, senior doctor, junior doctor and so on), a nurse (registered nurse, senior nurse, student nurse), laboratory technician, help desk assistant and a patient. These security levels for subjects will then be associated with different security levels defined for objects (EHRs), and thus access will be controlled using security levels.

Regardless of conceptually being considered feasible, the MAC implementation in a modern healthcare environment is likely to be difficult. Its main restrictions comes from a large number of users expected to participate in a healthcare system, a wide range of data types, together with a desire to give patients access to their own records as specified in various legislations discussed in Chapter 4 (Alhaqbani & Fidge, 2007). MAC is also inappropriate for dynamic environments since it is centrally controlled by a security administrator and users do not have an ability to bypass the already defined security policies. This actually conflicts with access control requirements for the domain which is witnessing a large number of unexpected access requests.

Role-Based Access Control

The past two decades have witnessed a huge explosion in research on RBAC. In academia, for example, a great number of papers on Role-Based Access Control (RBAC) have been published and the general approach has been adopted as a standard for security management in commercial organisations (David & Richard, 1992), (Sandhu *et al.*, 1996), (Sandhu *et al.*, 2000), (Ferraiolo *et al.*, 2001), (Joshi *et al.*, 2005). The industry's interest on RBAC has increased dramatically with major IT vendors offering products that incorporate some form of RBAC such as an Windows Authorisation Manager (AzMan) by Microsoft, which was first released in Windows Server 2003 (Microsoft, 2005). The AzMan framework is now used in Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2 and Windows Server 2012. There is also a Tivoli Security Policy Manager by International Business Machines (IBM, 2012), among others.

Despite being widely researched, adopted and used, RBAC is criticized for its inflexibility towards applications that require context information to be interpreted in real-time before making access decisions (Huang *et al.*, 2006). Specifying context information in RBAC may result in role explosion since each context information requires a definition of a new role and an accompanying permission(s) thus resulting in thousands of roles and permissions. Furthermore, pretty much all security measures in RBAC can be overridden by the use of emergency access features, which are extensively used in everyday work in health facilities. With its inflexibility, RBAC alone cannot ensure the continuity of care when implemented in a modern healthcare environment. This thesis, therefore, extends the traditional RBAC model with contexts and obligations in order to allow health workers to bypass access policies in an accountable manner in case of unexpected access requests.

Attribute-Based Access Control

In recent years, ABAC has drawn more attention as an approach which facilitates EHR accessibility due to its ability to authorise privileges based on attributes of subjects, objects and the environment. This specification of access rights based on attributes facilitates fine-grained access control policy administration per each individual subject. Contrary to RBAC, ABAC does not require separate roles for relevant sets of subject attributes, and hence, access rules in ABAC can be implemented quickly to cater for dynamic changing needs of the environments (Karp *et al.*, 2009). In other words, ABAC's approach made it easy to include context information in access control decisions.

As a trade-off to its flexibility, ABAC suffers from complexity associated with the number of cases that need to be considered for the model. As pointed out by Karp *et al.* (2009), for n attributes or conditions using attributes, there are 2^n possible combinations. Another major challenge of implementing ABAC in a real domain is that, it suffers from the lack of agreed meaning of attributes that can be used in the model. Section discusses access control models that closely relates to the one proposed in this thesis.

3.5 Models Classification

This section discusses different ways of classifying access control models. This section is divided into two parts: Section 3.5.1 discusses the generic taxonomy proposed by this thesis, and Section 3.5.2 reviews access control models that are related to the one proposed in this thesis and then categorises them based on the proposed taxonomy.

3.5.1 Introduction

There are numerous ways of classifying access control models. To begin with, Ferraiolo *et al.* (1995) started their classification of access control models by grouping them into two main groups based on access restriction. The two groups are: Discretionary Access Control (DAC) (comprising of Discretionary Access Control (DAC) model) and Non Discretionary Access Control (NDAC), consisting of Mandatory Access Control, Role-Based Access Control and Attribute Based Access Control models, among others (Ferraiolo *et al.*, 1995), (Yuan & Tong, 2005). Unlike DAC where access is restricted based on discretion of the object's owner, all accesses to resources in NDAC are controlled by a security administrator and organisation's security policies. This group of classification is summarised in Figure 3.13.

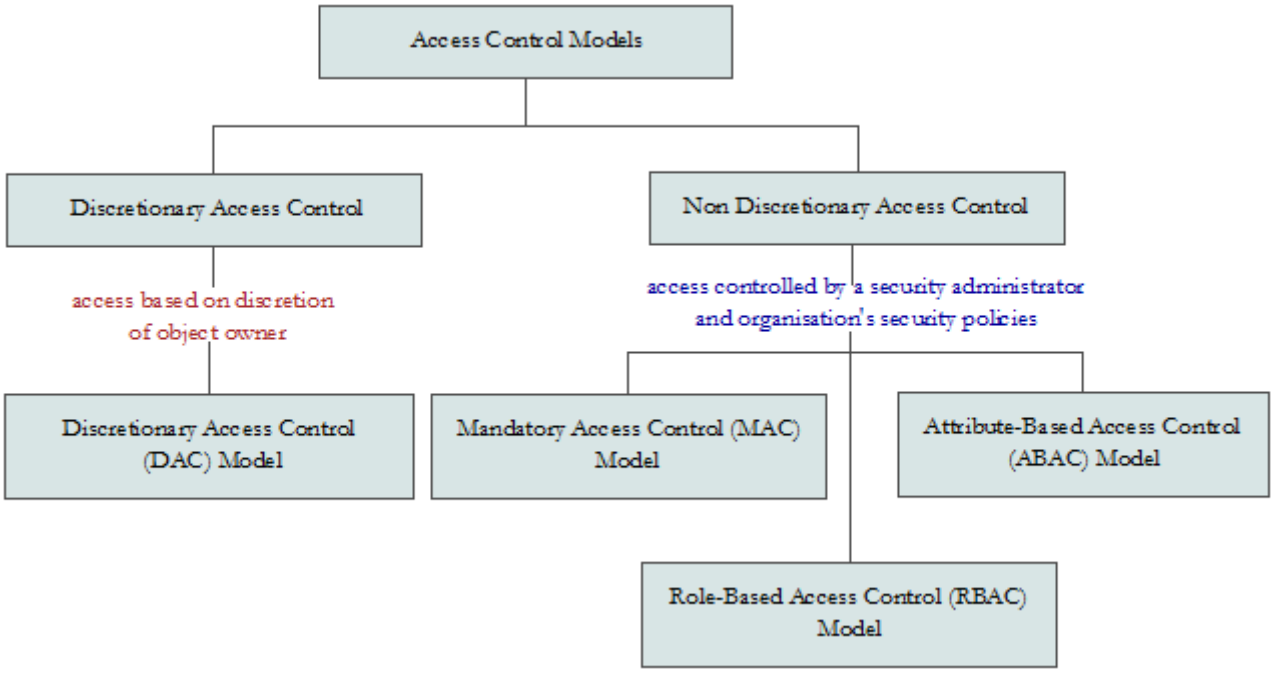


Figure 3.13: The classification of access control models by Ferraiolo *et al.* (1995)

There are more approaches for classifying access control models, as presented in Figure

3.14. These may include classification based on the type of information used

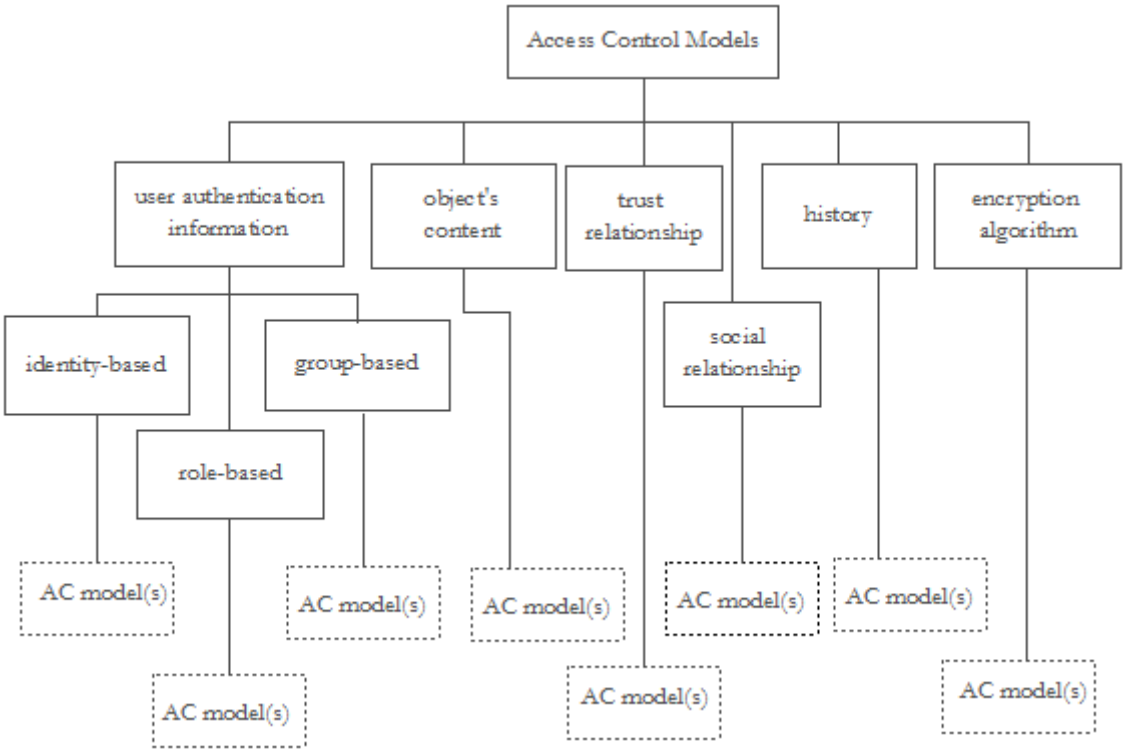


Figure 3.14: More approaches for classifying access control models (Source: Author)

for user authentication; which may include identity-based (Gong, 1989), role-based (David & Richard, 1992)) or group-based access controls models(Kalam *et al.*, 2003). They may also be classified based on the content of protected object, also known as content-based access control (Giuri & Iglio, 1997), (Guarino *et al.*, 1999), trust relationship between resource owner and a requester (also referred as trust-based access control) (Tran *et al.*, 2005), (Almenárez *et al.*, 2005) and user's social relationship (social-based access control) (Gollu *et al.*, 2007). Other distinguishing characteristics of access control models may include selective history of access control requests made by individual programs, called history based access control (Edjlali *et al.*, 1998), (Abadi & Fournet, 2003), (Fong, 2004) as well as encryption mechanisms used (Goyal *et al.*, 2006), (Wang *et al.*, 2006). This thesis extends on the work carried out

by Ferraiolo *et al.* (1995) as a base towards further categorisation of access control models discussed in Section 3.5.2.

3.5.2 Related Work

Role-Based Access Control (RBAC) is a well-established access control model with widely-recognised advantages, and it is supported by a large number of software products and platforms (Sandhu *et al.*, 1996), (Lodderstedt *et al.*, 2002). The model addresses access control requirements of commercial organisations, through an introduction of the role concept (Sandhu *et al.*, 1996), (Ferraiolo *et al.*, 2003), (Ferraiolo *et al.*, 2004). In RBAC, permissions are attached to roles and users must be assigned to roles to get the permissions. A role represents specific task competency, such as that of a medical doctor, or it can embody the authority and responsibility (Sandhu *et al.*, 1996). Roles define both the specific individuals allowed to access resources as well as the extent to which those resources can be accessed. Permissions determine what operations can be carried out on resources under access control. A user must establish a session to activate a subset of roles to which the user is assigned. Each user can activate multiple sessions, however, each session is associated with only one user. The operations that a user can perform in a session depend on the roles activated in that session and permissions associated with those roles.

The RBAC model supports roles hierarchies that define an inheritance relationship between roles. To prevent conflict of interest that may arise in an organisation, RBAC allows the specification of static and dynamic separation of duty constraints. Several works exist in the literature that improve RBAC functionality for different application domains. This section discusses the research works that are closely related to the access control model proposed in this thesis, and particularly how RBAC can be extended with different concepts or notions to make the overall approach "context-based" or

"context-aware".

As part of RBAC's extensions, Sampemane *et al.* (2002) introduce a new access control model for active spaces. The authors define an active space as "a computing environment that integrates physical spaces and embedded computing software and hardware entities". The active space allows interactive exchange of information between the user and the space. Environmental aspects are adopted into the access control model for active spaces, and the space roles are introduced into the implementation of the access control model based on RBAC. The proposed model supports specification of both Discretionary Access Control (DAC) and Mandatory Access Control (MAC) policies. While DAC policies allow users to create and update security policies for their devices, the MAC policies allow system administrators to maintain the access matrix.

Covington *et al.* (2001) introduced a Generalised RBAC (GRBAC) model to help control access to private information and resources in ubiquitous computing applications. In fact, the GRBAC model extends the traditional RBAC model by incorporating the notion of object and environment roles. The environments roles differ from the subject roles in RBAC but they do have similar properties, including: role activation, role hierarchy and separation of duty. In the access control framework enabled by environment roles, each element of permission assignment is associated with a set of environment roles, and environment roles are activated according to changing conditions specified in environmental conditions; in this way, environmental properties such as location and time are introduced to the access control framework. In a subsequent work, Covington *et al.* (2002) describe the Context-Aware Security Architecture (CASA), which is an implementation of the GRBAC model. The access control is provided by the security services in the architecture. In CASA, security policies are expressed as roles and managed by the security management service, authentication

and authorisation services are used to verify user credentials and determine access to the system resources. The environmental role activation services manage environmental role activation and deactivation according to environment variables collected by context management services.

Temporal Role-Based Access Control (TRBAC) is another extension of RBAC, proposed by Bertino *et al.* (1996) and Bertino *et al.* (2001). This work adds a time dimension to the RBAC model. Its authors [Bertino *et al.*] introduce the concept of role enabling and disabling. Temporal constraints determine when the roles can be enabled or disabled. A role can be activated only if it has been enabled. Joshi *et al.* (2005) extend the Temporal Role-Based Access Control (TRBAC) model by proposing the Generalised Temporal Role-Based Access Control (GTRBAC) model. In this work the authors introduce the concept of time-based role hierarchy and time-based separation of duty.

Several other researchers have also extended RBAC to incorporate spatial information. To cope with spatial requirements, Hansen & Oleshchuk (2003) extend the conventional RBAC model and propose Spatial Role-Based Access Control (SRBAC) model. The SRBAC model utilizes location in security policy definitions. Another most important work in this regard is GEO-RBAC (Bertino *et al.*, 2005), which is probably the most expressive location-based access control model. The role activation is based on the location of the user. Consider the following as a usage example of GEO-RBAC in a real world where a user can acquire a role of a patient when in a hospital grounds and a role of a teacher when in a school compound. The GEO-RBAC model supports the notion of role hierarchies but does not deal with separation of duties. Another work incorporating spatial information is by Ray & Kumar (2006). In this work, authors analyse how each component of a traditional RBAC is influenced by location. The authors define their model using the Z specification language. The

Location-Based Access Control has been addressed in some other works not pertaining to RBAC including Leonhardt & Magee (1997), Hengartner & Steenkiste (2004), and Ray & Kumar (2006).

There are also other works that incorporate both location and time in to the traditional RBAC. The research work by Chandran & Joshi (2005) combines the main features of GTRBAC and GEO-RBAC. In their LoT-RBAC model, role is enabled by time constraints. A user can activate a role if such a role is enabled and an individual user satisfies location constraints associated with role activation. Another feature worth mentioning from their work is that, when a role is activated all permissions associated with such a role can be invoked. Kumar & Newman (2006) proposed the Spatial Temporal Role-Based Access Control model, that is suitable for pervasive computing applications. With their access control model, the authors show the association of each component of the conventional RBAC model with spatial-temporal information.

In addition to location and time, the traditional Role-Based Access Control (RBAC) model has also been extended using purpose information. Ni *et al.* (2007) proposed a purpose-based access control model for privacy protection. Their proposed model is based on the notion of purpose roles through which purpose is categorised into intended purposes and access purposes. In addition to role attributes and system attributes, Ni *et al.* (2007) also incorporate purpose hierarchy into their model. However, despite its major contribution, the proposed access control model does not deal with other vital privacy-aware elements, such as obligations and complex conditions such as providing access for unexpected situations, that form an essential part of privacy protection.

RBAC can also be extended by the notion of trust. Bhatti *et al.* (2005) proposed a trust-enhanced version of their XML-based access control (X-RBAC) framework for web services. The proposed model, which is an extension of RBAC with trust

and contexts, incorporates context-based access control. Chakraborty & Ray (2006) propose a trust-based access control model called TrustBAC. The model extends the conventional role-based access control model with the notion of trust levels. Users are assigned to trust levels instead of roles based on a number of factors, including user credentials, user behaviour history, and user recommendation, and trust levels are assigned to roles which are assigned to permissions.

With these and other research works in access control, as summarised in Figure 3.16, this thesis argues that, to gain full advantage of contexts in an access control solution, the proposed access control system should incorporate context conditions that are specific to the application domain. In this case, RoC-BAC is designed by extending the traditional Role-Based Access Control (RBAC) model with the notion of health-related contexts, from a chosen study domain.

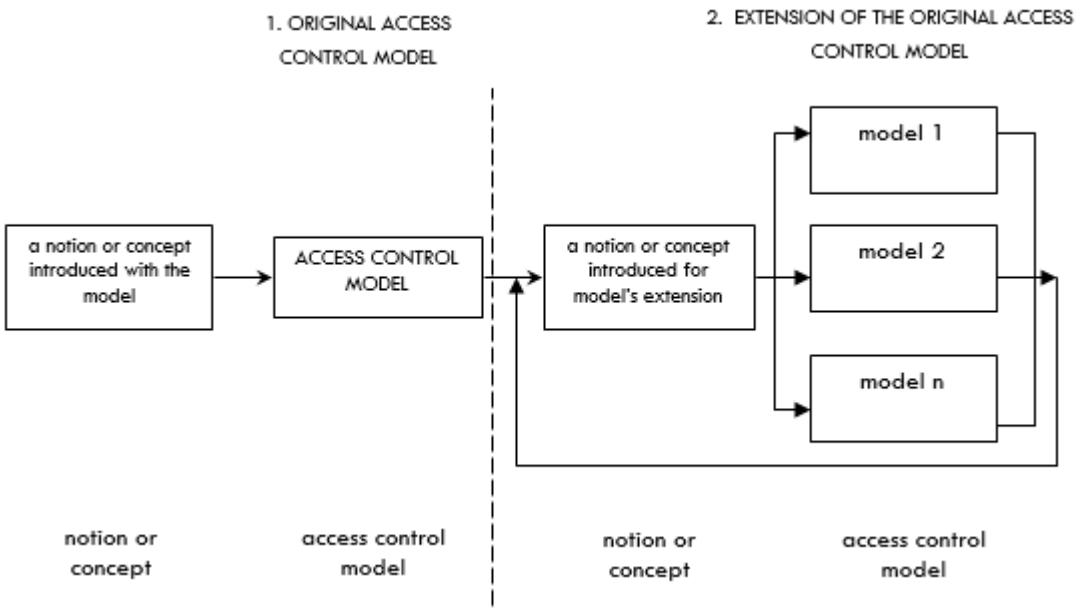


Figure 3.15: A summary of the taxonomy to classify access control models (Source: Author)

Figure 3.15 presents a taxonomy that can be used to classify access control models. Two main steps have been designed to enable classification of access control models.

These are: 1. identifying the original access control model and 2. checking whether that model has been extended or not, by identifying the notion or concept for an extension as well as the original access control model. These steps are numbered 1 and 2. The classification begins with the decision to design an access control model for a specific application or domain. Usually, this is done by proposing a notion or concept (for instance, security levels in Mandatory Access Control (MAC), designed for government and military applications, and role concept in Role-Based Access Control (RBAC), for large commercial organisations. In this thesis, access control models from the first step are referred as "original access control models".

The second step involves checking whether the original model has been extended or not. Similar to the first step, this can be done by identifying a notion or concept (marked with a dotted rectangle) together with its proposed model. If there is a new access control model that has been designed, then that notion with its related access control model are noted. The final step involves checking whether the extended access control model has been extended again. This process should be repeated until all the access control models and their extensions have been noted in a hierarchy-style classification. Figure 3.16 presents a taxonomy of access control models, with the new RoC-BAC model included. The full list of papers used in the taxonomy are in Appendix E.

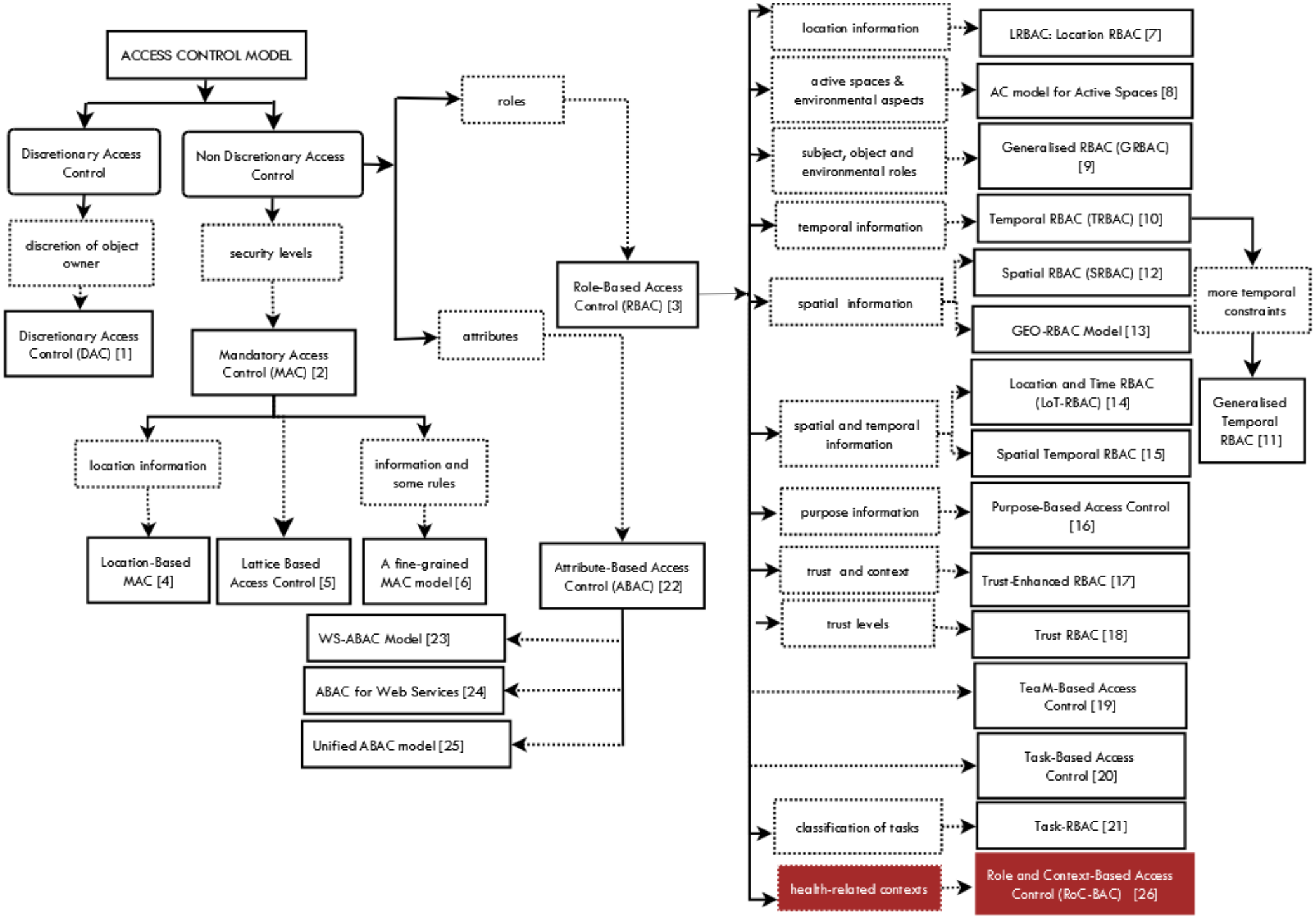


Figure 3.16: Taxonomy of Access Control Models with RoC-BAC included (Source: Author)

3.6 Conclusions

This chapter has provided an overview of the basic terms and concepts that are commonly used in access control research together with a discussion of well-known traditional access control models, including Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). The chapter also presents the researcher's findings from an analysis of the suitability of traditional models on modern healthcare environment. The existing literature indicates that, DAC is not suitable for modern healthcare environments, since the model is static, and lacks proper control of information flow where an owner of a particular object can pass access rights on that object to any other subject without restrictions. Discretionary Access Control (DAC) is, however, suitable for commercial applications where such lack of control on information flow may be tolerated. MAC, on the other hand, provides a rigorous control of information flow that is required in military and government applications. In fact, access control decision making in both DAC and MAC models assign static permissions to roles while a modern healthcare environments require contexts in its access decision in order to support the continuity of care.

To overcome the limitations of DAC and MAC usage in commercial organisations, RBAC was introduced. RBAC is a flexible and policy-neutral approach to access control, and it has generated great interest in the security community. Despite its success, RBAC cannot cope with the fundamental requirement of accommodating contexts in access control decision making. Incorporating contexts into RBAC may result into role explosion as each context requires a definition of a new role and an accompanying permission(s), henceforth resulting into hundreds of roles and permissions. To address the limitations of RBAC, a new generation of access control model called Attribute-Based Access Control (ABAC) was introduced. The approach uses

attributes to describe access requests and defines access control rules. The ABAC approach suffers from the complexity associated with the number of cases that need to be considered for the model, whereas for n attributes, 2^n cases needs to be considered. For as much as 10 attributes that might need to be considered, these makes 1,024 cases. This thesis, henceforth, proposes a new context-based access control model that accommodates infrequent access requests associated with emergency situations in the healthcare domain. Chapter 4 discusses generic access control requirements for the Tanzania healthcare domain.

Chapter 4

Access Control Requirements for Tanzania Health System

In this chapter access control requirements for the Tanzania healthcare system are discussed. These requirements are the by-products of a new methodology called COIL developed purposely to gather comprehensive access control requirements for the healthcare domain. The rest of this chapter is organised as follows. While Section 4.1 discusses research works that explore different aspects of access control requirements for the healthcare domain, Section 4.2 discusses four categories of access control requirements that forms the COIL (Contexts, Organisation rules, e-health Initiatives, Legislative rules) methodology. COIL methodology is discussed in Section 4.3, and a conclusion of the chapter is in Section 4.4.

4.1 Related Work

This section discusses different approaches to access control requirements in the healthcare domain.

To the best of the researcher's knowledge, there is no previous work that solely proposes a methodology for gathering comprehensive access control requirements for the healthcare domain. There are, however, research works that elicit some parts of access control requirements for the healthcare systems by other means. In a short, one page paper from 1998, Beznosov (1998) discusses requirements for access control in the United States of America's (USA) healthcare sector. He proposed access in the healthcare system to be based on affiliation (that is, subsidiary of the healthcare system a particular caregiver works for), role (representing a job function that a particular user is assigned in a current session), location (where does an access request comes from), time (as its name suggests, which is an important factor for users assigned to shift-related positions, like nurses and medical doctors) and relationships (representing a relationship between the user and the patient whose records are to be accessed). It was, however, not clear from the one-page paper where these conclusions on access control requirements came from.

Anderson (1996) discussed a general security policy model for clinical information systems, which includes access control. Motivated by the lack of a comparable security policy model that spells out clear and concise access rules for a clinical information systems, Anderson designed a security policy model in a form that is similar to the Bell-LaPadula model (Bell & LaPadula, 1973) for military systems and the Clark-Wilson model (Clark & Wilson, 1987) for banking systems. The proposed security policy was based on the rules set out by the British Medical Association (Sommerville & Horner, 1993), which incorporate much clinical experience, General Medical Council (2001),

and General Medical Council (Great Britain) (2006). Moreover, Blobel (2004) published a paper describing a set of models for authorisation management and access control in healthcare systems. The access control requirements proposed resulted from the researcher's experience and involvement in international EHR architecture and security standards, including Health Informatics - Electronic Health Record Communication (CEN ENV 13606) standard, Health Level Seven (HL7) - for exchange, integration, sharing and retrieval of electronic health information and CORBA (a standard designed to facilitate communication of systems that are deployed on diverse platforms).

Evered & Bögeholz (2004) published a paper describing how they performed a detailed case study on access control requirements in a small aged-care facility in Australia which at the time of the study the facility used paper-based records. Their study concluded that access control requirements are very complex even for a small healthcare facility. To address the lack of research works on access control requirements for healthcare systems, Rostad & Edsberg (2006) conducted a study on access control requirements in the healthcare systems in Norway. Their access control requirements were based on audit trails from access logs. One significant observation from this study was that exception-based access control mechanisms were frequently and widespread used. To minimise their usage in healthcare systems, Rostad & Edsberg (2006) proposed a structured and fine-grained logging and analysis of access logs. Alhaqbani & Fidge (2007) investigated appropriate access control requirements for processing electronic health records. The researchers pointed out that "access to sensitive patient data needs to be accessible by authorised personnel when needed and also available in life-critical situations". They also claimed that no single access control model is sufficient in a federated healthcare environment, but rather the required level of data security can be achieved through a judicious combination of three different mechanisms.

There have also been various research papers mentioning different access control requirements for healthcare systems. Among others are: Motta & Furuie (2003) who proposed a contextual role-based access control authorisation model for electronic patient records. The proposed model, which regulates user's access to electronic patient records, is based on organisational roles and was aimed to increase patient privacy and confidentiality of their data. Bacon *et al.* (2002) designed a model named OASIS Role-Based Access Control which satisfies context-sensitive access control requirements in large-scale systems, such as the national EHR service.

Based on the review of both related research works and projects, in this thesis, access control requirements for the healthcare domain are grouped into four. These are: contexts, organisational rules, privacy and security capabilities from national e-health initiatives as well as legislative rules. As a first step towards the development of a new methodology for gathering comprehensive access control requirements for the Tanzania healthcare system, Section 4.2 discusses each single component from the four parts that form the COIL methodological approach.

4.2 Access Control Requirements

This section discusses four elements of access control requirements for the healthcare domain. The items discussed include: contexts, organisational rules, national e-health initiatives, and legislation and regulations.

4.2.1 Legislation and Regulations

The privacy and security of patient health information is a top priority for patients and their families, healthcare professionals, healthcare providers and the government as a whole. To protect personal health information from unauthorised access and use, leg-

islation requires responsible individuals and organisations that collect, process, store, use and transfer patient health information (either paper-based or electronic) to have access rules, security policies and other safeguards in place. This section, henceforth, analyses different parts of legislation in relation to access to electronic medical records so as to identify access control requirements for the Tanzania healthcare system. The legislation discussed herein include the Health Insurance Portability and Accountability Act (HIPAA) from the United States of America, the European Union Data Protection Directive for member states of the European Union and data protection in Tanzania.

4.2.1.1 Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a "multifaceted law designed to protect the security and privacy of medical information, and yet to enhance the ease of use with which they can be shared between entities" (Nanda & Burleson, 2003). It was initially introduced by the Congress as the Kennedy-Kassebaum Bill (Starr, 1996) and enacted as the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, in August 21, 1996. HIPAA has two main goals:

i. Health Insurance Portability: to ensure that individual citizens would be able to maintain their health insurance between jobs and

ii. Accountability: designed to maintain security and confidentiality of patient health information. The HIPAA Act also mandates uniform standards for electronic data transmission, both financial and administrative, which relates to patient health information (HIPAA, 1996)

These objectives were pursued through three main provisions of the Act, namely: i. portability ii. tax, and iii. administrative simplification provisions. The access control requirements are on the HIPAA Privacy Rule, which is promulgated under the third

provision.

HIPAA incorporates four health information standards addressing administrative simplification. These standards (including transaction and code sets, privacy rules, security rules and national provider identifier) have been adopted by the United States Department of Health and Human Services (HHS). The requirements presented in this section have been extracted from the HIPAA (1996) and Borkin (2003), and which have been further explained in Health Information Technology for Economic and Clinical Health (HITECH) Act (HITECH, Feb 17, 2009).

1. **Applicability**

   Under Section 1172 of HIPAA, the HIPAA privacy rule and administrative simplification rules apply to:

   - Health Plans: include individual and group plans that provide or pay the cost of medical care. These may include employer-sponsored group health plans, health insurance companies, government and church-sponsored health programs.

   - Healthcare Providers: include every healthcare provider, regardless of the size, who electronically transmits health information in connection with certain transactions. This category applies to both institutional healthcare providers like hospitals and non-institutional providers like physicians, dentists, psychologists, pharmacies and other practitioners.

   - Health care clearinghouse: refer to public or private entities, including a billing service, repricing company, community health management information system, and "value-added" networks and switches, that either process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into

standard data elements or a standard transaction or vice versa (that is, receives a standard transaction from another entity and processes or facilitates the processing of health information into a nonstandard format or nonstandard data content for the receiving entity)

2. **Protected Information**

   The privacy rule protects all "individually identifiable health information" held or transmitted by applicable entities, in any form or medium, whether electronic, paper or oral.

   The "individually identifiable health information" is information, including demographic data, that relates to

   - the individual's past, present or future physical or mental health or condition
   - the provision of health care to the individual, or
   - the past, present, or future payment for the provision of health care to the individual

3. **Healthcare Professionals' Responsibility**

   (a) Disclosure of Identifiable Health Information

   Section 1177 (a) OFFENSE - A person knowingly and in violation of this part

   - Uses or causes to be used a unique health identifier
   - Obtains individually identifiable health information relating to an individual
   - Discloses individually identifiable health information to another person and in turn that person should be punished. The punishment may

range from monetary fines (between $50,000 to $250,000) to imprisonment (between 0 and 10 years).

(b) Minimum Necessary Access

HIPAA Privacy Rule requires covered entities to establish, develop and implement reasonable policies and procedures that limit protected health information with minimum access to achieve purpose of disclosure.

4. **Patient Rights and Consent**

(a) Individual Access

One of the main access control requirements that is crucial in the healthcare domain is an ability to allow individual patients to access their protected health information. With some exceptions, the HIPAA Privacy Rule allows individuals to have rights to review and obtain copies of their protected health information in a covered entity's designated record set. Among the circumstances excluded from the rule include: physiotherapy notes, information compiled for legal proceedings and laboratory tests to which certain legislation prohibits its access.

(b) Personal Representative

In relation to uses and disclosures of the individual's protected health information, HIPAA Privacy Rule requires covered entities to treat a personal representative (or a parent in case of a minor patient) in the same way as the individual patient whose information is being processed. A personal representative is formally defined as a person who is legally authorised to make healthcare decisions on behalf of the concerned individual.

(c) Patient Consent

To disclose protected health information for other than the intended origi-

nal purpose (treatment, payment or other healthcare operations), covered entity must obtain individual's written authorisation.

5. **Access Control**

   Section 164.312 (a)(1) of HIPAA Security Rule defines two requirements for access control (Department of Health and Human Resources, 2007), including

   (a) Unique User Identification - each user should be assigned a unique username or number for identifying and tracking user identity.

   (b) Emergency Access Procedure - For emergency access requests, healthcare providers are required to determine types of situation that would require such an access to information system or application that contain EHRs.

4.2.1.2 European Union Data Protection Directive

The European Union Data Protection Directive regulates collection, processing, storage, use, disclosure and transfer of personal data within the European Union (European Union, 1995), (Bennett & Raab, 2003). The directive was introduced in 1998 in order to protect the fundamental rights and freedom of people, and in particular their rights to privacy, in respect to the processing of personal data. It also incorporates numerous policies and mechanisms that attempt to closely track the flow of information. That is wherever, (European) personal data flows, there should be adequate legal protection of that data (Birnhack, 2008).

To standardize the protection of data privacy in Europe, the European Union Data Protection Directive contains the following requirements:

- Individuals must have access to their personal information and be able to correct them. There must also be mechanisms to assure compliance with the directive; recourse for individuals who are affected by non-compliance and consequences

for organisations when the directive is not followed.

- An organisation must inform individuals about purposes for which it collects and uses information about them, and types of third parties to which it discloses that information.
- Corporations and governments are forbidden from using virtually any personal records for any purpose other than the original one, without explicit permission.
- An organisation must offer individuals an opportunity to opt-out whether their information can be used for purposes other than the one for which it was purposely gathered. For sensitive information such as medical conditions, racial or ethnic origin, political opinions and so on, consumers must be given specific opt-in choice before information is disclosed to third parties.
- Personal data on European Union citizens may only be transferred to countries outside the 28-nation block that adopt these rules or are deemed to provide "adequate protection" for such data

Although both HIPAA and European Union Directive were enacted to protect patient health information, there are striking similarities and differences that exist between the two. While both legislation recognise that health information belongs to an individual who is the subject of that information, HIPAA asserts that healthcare provider is the owner of the information and the law grants some interest and rights over the information to the patient (Roach, 2006). In Europe, however, this approach is not plausible since ownership of health information is entirely granted to the patient and the healthcare unit is designated as either a controller or processor with legal rights, interests and obligations over the information.

4.2.1.3 Data Protection in Tanzania

To-date, there is no effective regime on data protection from individuals whose personal data is subjected to some form of automated processing on both Tanzania mainland and Zanzibar. The absence of data protection law is, in fact, a heavy loss to citizens as it exposes them to breaches of privacy, and also pose some great threats on misuse of information and data. On a positive note, Tanzania is in the initial stages of drafting new cyber security laws to combat cyber-crimes (Tanzania Online, 2012). In creating such laws, the Data Protection and Piracy Act will become the main piece of the legislation and the Computer and System Act and Electronic Transaction Act will follow (ITNews, 2013). In relation to collection, processing, storage, transfer and use of electronic patient information, these laws are expected to strengthen the electronic healthcare regulatory environment and create a foundation for specific electronic healthcare regulations. Section 4.2.1.4 summarises rules from selected legislation and regulations designed to govern privacy and security of patient health information.

4.2.1.4 Legislative Rules

This section summarises rules from legislation and regulations designed to ensure privacy and security of patient health information. They form a first category of the COIL methodology.

L1. Patients' medical data should only be collected and processed by healthcare professionals or individuals who are working on their behalf (known as data processors in the European Directive on Data Protection).

L2. The purpose(s) of medical data collection and processing should be defined before any transactions. Any changes in the original purpose should be communicated to a data subject.

L3. In normal circumstances, healthcare professionals must obtain permission (known as consent) from patients before undertaking any medical procedures.

L4. An individual patient should be allowed to appoint a representative who will be allowed to access medical data on his or her behalf. The representative should be treated in the same way as an individual whose information is being processed.

L5. A patient should be allowed to access their medical data either directly, through a healthcare professional, or through a representative, as permitted by law.

L6. Patients may request to review and rectify errors concerning their medical data.

L7. In any circumstance, correspondence between patient and a healthcare professional should remain private.

L8. Access to medical data may be refused, limited or delayed, if restricted by law.

L9. There should be policies, legislation and procedures that restrict, control or hamper patients access to information and services via the Internet and other communication media.

L10. Appropriate measures (administrative, technical and physical) should be implemented so as to prevent medical information from unauthorised access and modification.

L11. To deal with emergency access, which is part of infrequent access requests, healthcare providers are required to determine types of emergency situation that would require access to information system or application that contain Electronic Health Records (EHRs).

L12. Policies and procedures that limit protected health information with minimum access to achieve the intended purpose should be developed and implemented.

L13. To enforce accountability, a posteriori mechanism should be available in order to

establish who has accessed the system, what type of medical records have been accessed and when.

L14. There should also be internal legislation and organisational rules from healthcare organisations. These rules should govern operations and procedures to protected medical records.

These fourteen rules were then sent to ten experienced healthcare professionals working in different healthcare facilities in Tanzania to check for their appropriateness for the domain. The experts involved in evaluation of legislative rules were recruited using the snowballing approach and they were asked two questions: The first question they were required to go through the provided legislative rules (L1 to L14) and specify whether they are appropriate for the domain or not.

Table 4.1: Evaluation of Legislative Rules by Expert Users

Rule No.	EU 1	EU 2	EU 3	EU 4	EU 5	EU 6	EU 7	EU 8	EU 9	EU 10
L1										
L2										
L3	✓		✓	✓		✓	✓	✓		
L4										
L5										
L6										
L7										
L8										
L9										
L10										
L11	✓		✓	✓		✓	✓	✓		
L12	✓		✓	✓		✓	✓	✓		
L13	✓		✓	✓		✓	✓	✓		
L14										

EU abbreviation for an Expert User
L1- L14 denotes legislative rules number L1 to L14

With the second question, users were required to point out legislative rule(s) from the list provided that they consider appropriate for the domain. While all ten experts agreed that these legislative rules were appropriate for the domain, six of them pointed out rules L3, L11, L12 and L13 as the ones to be implemented in a new system, as shown in Table 4.1. Four of the experts did not comment on their choice of rule(s) for the implementation in a Tanzania health system. From these results, the following are considered as appropriate access control requirements that should be adopted in a Tanzania health care system. These include:

1. Patient Consent: It refers to permission given by a patient to a health care worker in relation to sharing and accessing the patient's health information.

2. Emergency Access Procedure: There should be a mechanism to support emergency access procedures (that are part of infrequent access requests), and which are common in healthcare settings.

3. Minimum Access: In order to support the continuity of care, healthcare professionals should be given minimum access to protected health information in case of infrequent access requests

4. Accountability: There should be mechanisms implemented in a system to allow an enforcement of accountability.

4.2.2 National E-Health Initiatives

In this section, documents from selected national electronic health initiatives are explored, and privacy and security capabilities are presented. The capabilities from this section form the second category of the COIL methodology.

4.2.2.1 National Programme for Information Technology

The United Kingdom National Programme for Information Technology (NPfIT) in National Health Service (NHS) was a ten-year programme established in 2002, and presented an unprecedented opportunity to use Information Technology to reform the way NHS uses information. The NPfIT was estimated to connect more than 100,000 doctors, 380,000 nurses and 50,000 other healthcare professionals and, it was expected to hold life-long records of fifty million residents in the United Kingdom, and thus improve healthcare services and quality of care to patients (Granger *et al.*, 2004), (Becker, 2007).

The core programme in NPfIT was the National Care Record Service (NCRS), which was aimed to make relevant parts of patient clinical records available to whoever needed so as to take care of a patient. The NPfIT contained other services including: Electronic Appointment Booking, Electronic Transmission of Prescriptions and NHS network (Brennan, 2009), (National Audit Office, 2009). The NCRS, for instance, was designed to enable each patient's detailed records to be shared securely between different parts of the local NHS such as General Practitioners and hospitals. More importantly, NCRS was expected to allow patients to have summary of their important information, named Summary Care Records, available to authorised health professionals at any NHS location.

The capabilities of the NPfIT are discussed in the Spine infrastructure (NHS, 2012), and they contain the following

- Unique Identifier: The NPfIT uses a single unique NHS number for every patient to facilitate safe, efficient and accurate sharing of patient information across organisational and system boundaries, within the NHS.
- Summary Care Record (SCR): It is an electronic record which contains informa-

tion in a summary form of a patient including medicines that a patient takes. SCR are useful for healthcare professionals involved in providing care to patients in an emergency or out-of-hours service with faster access to key clinical information.

To ensure confidentiality of patient data, NPfIT includes

- Authentication
- Role-Based Access Control (RBAC)- for authorising system functions and data,
- Legitimate Relationships with Audit and Alerts- for authorising user accesses to patient records as well as,
- Patient consent for sharing personal sensitive information

These services are provided through the application of information governance processes (Monitor, 2008), (Tett, 2010).

Despite huge investments (nine years and £11.4 billions), the Department of Health (DH) has failed to deliver the universal NCRS, and NPfIT has been dismantled (Parliament, 2011). The DH has, however, adapted an alternative approach whereas NHS trusts are now expected to develop smaller, regional networks of EHRs that are compatible with the programme. The implementation of this alternative approach means different parts of the country will have different systems and hence resulting in interoperability problems. Similar to issues faced by NPfIT, the implementation of the alternative approach has already fallen significantly behind schedule and the cost has escalated.

The House of Commons (2009) lists the following as the problems of NPfIT, among others

i. Difficulties in gaining acceptance and support from NHS staff and the overall

public

ii. Lack of cost-benefit analysis of the programme and other mini-programmes

iii. Difficulties in adhering to the project plan and schedules due to continuing delays and history of missed deadlines

iv. Poor integration of clinicians and other NHS staff into the project, and

v. Disagreement on confidentiality approach, and concerns on data security.

4.2.2.2 National Electronic Health Record - Singapore

In its 2006 report on ageing population, the Singaporean government estimated that by the year 2030, the country will witness an unprecedented profound age shift as the number of residents aged sixty five and older will increase from 300,000 to 900,000 (Committee on Ageing Issues, 2006), (Ministry of Health, 2012). In other words, these statistics reflect that one out of every five residents will be a senior by the year 2030. To cope with the ageing population, the government established a National Electronic Health Record (NEHR) in 2009 with the vision "One Singaporean, One Health Record", to allow patients to move seamlessly within an integrated care system.

The NEHR was established in order to enable electronic patient health records to be shared across the country's healthcare system, and thus to reduce waiting times and to provide better management of quality and cost of healthcare for its 5.1 million population. Unlike NPfIT initiative which was dismantled after failing to achieve its intended goal, the first phase of Singapore's $144 million NEHR system went live in July 2011, and it was on schedule (Li, 2011), (Accenture, 2012).

The following are the authentication and authorisation capabilities from the NEHR, as discussed by Accenture (2012):

- National Health Identification Service (NHIS): NHIS is a patient master index that enables EHR to match patient records received from across the domain. It enables healthcare providers to uniquely identify people through a combination of factors including national identifier, birth date, physical address together with other demographic information.
- Summary Care Records (SCR): NEHR delivers a SCR of each patient, and it incorporates a concise overview of most recent clinical activities of an individual including problem lists, medications and event summaries.
- Privacy and Security: To ensure privacy and security to patient data, NEHR incorporates role-based access, data sensitivity classification and Break-The-Glass functions that enables physicians to access patient information outside normal privacy and security settings.
- Audit and Logging: The system contains full audit logging capabilities that capture who has accessed what information, when, where and how.

4.2.2.3 HealthConnect - Australia

The National E-Health Transition Authority (NEHTA) is a not-for-profit organisation established by the Australian governments (both state and territory) with the intention to develop "better ways of electronically collecting and securely exchanging" health information (Jalal-Karim & Balachandran, 2008). NEHTA's fundamental goal is to develop a standardised, shareable EHR that is readily available and can be transferred more quickly and securely between healthcare professionals, who are authorised by the patient to access such information. Australia's National EHR system is known as HealthConnect, previously known as National Health Information Network (Gunter & Terry, 2005).

As discussed in NEHTA's blueprint, HealthConnect includes the following capabilities (National E-health Transition Authority, 2011):

- National Unique Identifier: This is a single identifier which is used to identify patients within HealthConnect.
- Summary Care Records: Patients who choose to participate in the system will have summaries of their health records stored in electronic form in one or more networked databases.
- Privacy and Security: HealthConnect uses a multi-layered approach to maintain privacy and security of patient information. There are several technical and non-technical controls which have been identified in NEHTA's blueprint, including (i.) smart cards - to facilitate accurate identification and authentication, (ii.) Role-Based Access Control policies, and (iii.) audit trails and monitoring access.
- Access to Health Information: HealthConnect enables healthcare providers (with a support of a patient consent) to access summary care information on all of patient interactions with the healthcare system. This enables healthcare providers to search medical records quickly and easily. Similarly, patients are be able to access their health information from multiple healthcare providers, through a single HealthConnect access point.

4.2.2.4 National e-Health Strategy - Tanzania

As noted earlier in Section 4.2.1.3, Tanzania has no legislation that controls the collection, processing, storage, use, and transfer of electronic healthcare information. This has resulted in a fragmented landscape of ICT pilot projects, and information system silos with significant barriers to achieve effective sharing of information between healthcare participants (MoHSW, 2013c). In addition, the Tanzania health care sys-

tem faces a risk of continued duplication, ineffective expenditure and creation of new solutions that cannot be integrated or scaled across the continuum. To address these issues, the MoHSW decided in 2009 to develop a national e-health strategy (officially published in 2013) to guide the use of ICT in supporting the transformation of the healthcare sector (MoHSW, 2013c).

The following capabilities has been specified in the National e-Health Strategy

- Tanzania Health Enterprise Architecture

    1. In a strategy document, the MoHSW adopts an Enterprise Architecture as a framework to guide the development of the National Health Information System (NHIS). The NHIS is a collection of interconnected (loosely or tightly) information systems that support healthcare operations, management and decision making in the healthcare sector.

    2. Another significant capability specified in the strategy document is the realisation that integrated NHIS requires a long term plan that builds from existing solutions. This capability is one of the reasons behind this decision to extend the traditional Role-Based Access Control (RBAC) model with contexts and obligations so as to support the continuity of care.

- Privacy and Security:

    1. The implementation and use of e-health solutions must place the highest importance on protection of patient information to guarantee privacy and integrity.

    2. The strategy points out on the need to establish privacy and regulatory framework to guarantee that privacy safeguards and consent processes for access and use of health information are followed by healthcare organisations.

3. The strategy document also states that the implementation of a national e-health strategy should converge on fewer and more reusable, cost effective ICT systems that are extensible, scalable and manageable.

Similar to electronic health initiatives from other countries, the implementation of a national e-health strategy in Tanzania is expected to address significant challenges including the shortage of qualified human resources for health which is the source of inefficiencies in the overall healthcare system. If the shortage of healthcare workers is successfully addressed through the use of ICT, the Tanzania's healthcare system will be in a position to support the continuity of care to patients. Section 4.2.2.5 summarises capabilities from national e-health initiatives against those considered appropriate for the Tanzania healthcare system.

4.2.2.5 Capabilities from National E-Health Initiatives

This section summarises privacy and security capabilities extracted from selected national electronic health initiatives.

The capabilities discussed herein form a second category of the COIL methodology, and they can be used as a guideline while designing a context-based access control system for the domain where infrequent access requests that involve emergency situations are common. From a summary of capabilities in Table 4.2, the National Electronic Health Record (NEHR) in Singapore specifies the need for healthcare information systems to implement authentication mechanisms (using a combination of username and password, or any other means) to confirm the user requesting access to protected records is the one specified in the system. For authorisation, Role-Based Access Control is a preferred approach to specify access rights for health care workers, as well as other users accessing the system. The Break-The-Glass functions are specified to provide access for infrequent access requests (which is part of emergency accesses).

While patient consent is required to allow a patient to allow healthcare professionals to access their health information, auditing and logging is incorporated to enforce accountability in the system

Table 4.2: The summary of access control requirements from the national e-health initiatives

Capability	**National e-health initiative**				**Access Control Requirement Proposed in this Thesis**
	United Kingdom (NPfIT)	**Singapore (NEHR)**	**Australia (NEHTA)**	**Tanzania (e-Health Strategy)**	
User Identification and Authentication	Authentication	Authentication	Identification and Authentication	Authentication	Identification and Authentication
Authorisation	Role-Based Access Control	Role-Based Access Control	Role-Based Access Control	Role-Based Access Control	Role-Based Access Control
Emergency Access	Not specified	Break-The-Glass functions	Not specified	Not specified	Break-The-Glass
Auditing	Auditing and Alerts	Auditing and Logging	Audit Trials and Monitoring	Not specified	Auditing and Logging
Patient Consent	Required	Required	Required	Required	Required

From the data collected and observations on how health care workers operate, and how the current systems are used in a Tanzania healthcare system, this study makes a number of conclusions in case of privacy and security capabilities for the domain as shown in the right column of Table 4.2, labelled "Access Control Requirement Proposed in this Thesis". First and foremost, this study found that Role-Based Access Control is an access control mechanism implemented in most healthcare systems in Tanzania. This fact is well confirmed by a partial list of healthcare information systems discussed in Chapter 2, Section 2.4. The Tanzania healthcare system requires an implementation of functions similar to Break-The-Glass to provide infrequent access requests (emergency accesses is part of) in healthcare organisations. There should

also be identification and authentication so as to identify and authenticate users using the system, as well as auditing and logging procedures. Section 4.2.3 analyses what context is and categories of context for the healthcare domain.

4.2.3 Contexts

The main aim of this section is to introduce context, which forms the third category of the COIL methodology. The section begins with a discussion of what context is, followed by scenarios involving its usage in three different domains. The last part discusses how and which context will be used in this thesis in order to maintain the continuity of care by allowing an accountable sharing of personal information.

4.2.3.1 Context: Definition

Context as a concept has been studied by philosophers, linguists and psychologists (Allen & Shatz, 1983), (Winograd, 2001). In the last few years, however, its use in Computer Science has grown tremendously, spanning into a wide range of disciplines from information retrieval and reasoning in Artificial Intelligence to ontologies in Knowledge Representation (Bricon-Souf & Newman, 2007). In each such domain, context has been interpreted in a certain way that is well suited for their goal and thus making it an elusive concept to define (Henricksen *et al.*, 2002), (Bazire & Brézillon, 2005), (Wan, 2009). The main aim of this section is, therefore, to provide a brief review of what context is based on definitions proposed by researchers from different domains.

Initially, definitions of context were categorised into two main groups. These are: definitions that only provide examples of context information to define context, and those that state what context is, with or without examples. From the first category, Schilit & Theimer (1994) enumerate context as location of the user, identities

of nearby people and objects and changes to those objects over time. This definition is regarded as the first research work that introduced the term "context-aware". In a similar fashion, Brown *et al.* (1997) ascertain context as location, time of the day, identities of people around the user, orientation of the device, season of the year and temperature. Ryan *et al.* (1998) list user's location, identity and time. Additionally, Dey (1998) points out emotional state, focus of attention, location and orientation of the device, date and time of the day, objects and people in the users environment as context. Although authors of each of these definitions list context elements or variables, it is difficult to apply any of them if you need to determine the type of information not listed is actually a context or not (Dey, 2001).

The second approach towards context definition involves an analysis of selected definitions that state what context is, with or without context elements or variables. Salber *et al.* (1999) define context as any information that is part of an application's operating environment and such information can be sensed by the application. Salber *et al.* (1999) identify location, identity, activity and state of people, groups and objects, temperature and lightings as context for the buildings and rooms fitted with sensors. Likewise, Dey (2001) and Abowd *et al.* (1999) formalise context as "any information that can be used to characterise the situation of an entity. An entity is a person, place, or an object that is considered relevant to the interaction between user

Table 4.3: A Summary of Definitions of Contexts from Literature

No.	Author(s)	Context and Variables
1.	Schilit *et al.* (1994)	User's location, lighting, noise level, network connectivity, communication costs, communication bandwidth and social situation (whether you are with your manager or co worker)
2.	Brown *et al.* (1997)	Location, time of the day, identities of the people around the user, orientation of the device, season of the year and temperature
3.	Ryan *et al.* (1998)	User's location, identity and time
4.	Schmidt *et al.* (1999)	Human factors: user, social environment and task Physical environment: conditions (such as light, pressure, acceleration, audio and temperature), infrastructure, location and time
5.	Chen *et al.* (2000)	User's profile, user location, time of the day, nearby people and devices and user activity
6.	Satyanarayanan (2001)	Position, orientation, identities of the people nearby, locally observable objects and action, emotional and physiological state
7.	Ouchi *et al.* (2002)	Health conditions, movements and behaviours
8.	Miguel-Garcia *et al.* (2003)	User's location, delivery timing, role reliance and device location and state (such as temperature reading) and other artifacts (like availability of laboratory results)
9.	Zhang *et al.* (2005a)	Context has been categorised into five groups. Personal health context: pulse, blood pressure, weight, glucose level. Environment context: temperature, light, humidity and noise. Task context: goals, tasks, actions, activities. Spatial Temporal context: location and time Terminal context: screen size, colour, quality of the screen, energy type, operating system, interface, terminal type and media supported.
10.	Varshney (2007)	Pulse rate, User's actions and posture, Electrocardiogram (ECG), respiration rate, oxygen saturation, transmission of packets over wireless network
11.	Jung & Lee (2007)	Bio Signal context: ECG, respiration rate, oxygen saturation, blood pressure, body temperature, body sugar, body fat, weight Environment context: temperature, relative humidity, oxygen rate, wind speed and rain gauge
12.	Wood *et al.* (2008)	Location, pulse, blood pressure, ECG, room temperature, light levels, dust and user activities
13.	Bardram & Nørskov (2008)	Patient identification (including ID, name, social security number), allergies, patient current status and location, and location of the clinicians)

and application, including user and applications themselves". From his definition, Dey (2001) lists location, identity, time and activity as relevant context information in Ubiquitous Computing.

From their psychological study, Federenko *et al.* (2004) offer a simple and straightforward definition of the term context. They define context as a set of variables that define a situation. Similarly, Bazire & Brézillon (2005) define context as "a set of situational elements in which an object being processed is included". From a summary of definitions of contexts in Table 4.3, some researchers have specified healthcare-specific contexts. Among others, context variables specified include health conditions, movements and behaviours by Ouchi *et al.* (2002), user's location, delivery timing, role reliance, and device location and state by Miguel-Garcia *et al.* (2003).

Zhang *et al.* (2005a), on the other hand, categorise context into five groups, including personal health, environment, task, spatial temporal, and terminal contexts. Other definitions of context from researchers in healthcare are specified by: Varshney (2007), Jung & Lee (2007), Wood *et al.* (2008) and Bardram & Nørskov (2008). From the two categories of context definitions, this thesis adopts a simpler definition by Federenko *et al.* (2004) and categorises contexts in a similar fashion as Zhang *et al.* (2005a). The definitions of contexts are summarised in Table 4.3. Through further analysis of existing literature, more contexts were identified (as summarised in Table 4.4).

Using the categorisation proposed by Zhang *et al.* (2005a), initially contexts in this study were grouped into five categories: personal health contexts, terminal contexts, environment contexts, tasks contexts, and spatial temporal contexts , as shown in Table 4.4. Since the main aim is to design a new context-based access control model for infrequent access requests, contexts were then re-categorised to fit with the application domain. The new four categories of contexts used for the rest of this thesis are:

Table 4.4: Categorisation of Contexts (Source: Author)

Personal Health Context	Terminal Context	Environment Context	Task Context	Spatial Temporal Context
- Patient Identification including ID, name, social security number - Patient Allergies - Pulse Rate - Blood Pressure - Body Weight - Glucose Level - Respiration Rate - Oxygen Saturation - Electrocardiogram - Body Temperature - Body Sugar - Body Fat - Previous Diseases - Therapies - Operations - Current Symptoms - Already Available Diagnosis - Behaviours - Movements - Health Conditions - Patient Location - Patient Current Status - Personal Situation - Posture - Patient Activity - Location of the Clinicians - Identities of the People around the Patient	- Screen Size - Colour - Quality of the Screen - Energy Type - Operating System - Interface - Terminal Type - Media Supported - Orientation of the Device - Location of the Device - State of the Device - Nearby Devices - Communication Bandwidth - Communication Costs - Network Connectivity - Transmission of the Packets	- Temperature - Light Levels - Relative Humidity - Noise Level - Oxygen Rate - Wind Speed - Rain Gauge - Dust - Pressure Acceleration - Season of the Year	- Goals - Tasks - Activities - Actions	- Location - Time

subject contexts, object contexts, environment contexts and health-related contexts. The health-related contexts result from personal health contexts, with inclusion of contexts extracted from the Tanzania healthcare system.

4.2.3.2 Contexts: Tanzania Healthcare System

From Chapter 1, the main aim of this thesis has been to design a new context-based access control model for an infrequent access requests, using Tanzania's healthcare system as a case study domain. The proposed model should support the continuity of care to patients by allowing healthcare professionals to bypass access rules in an accountable manner. To achieve this, an implementation approach used in this thesis involves extending the traditional Role-Based Access Control (RBAC) model with contexts and obligations. This section, therefore, presents health-related contexts (resulting from Personal Health Contexts category in Table 4.4, Column 1) extracted from the Tanzania healthcare system.

The following health-related contexts were collected from healthcare professionals working in different facilities in the Tanzania's healthcare system. These contexts were then verified by checking in a list of crimes and road accidents published by the National Bureau of Statistics (NBS, 2013)

1. **Ministry of Community Development, Gender and Children**

   The contexts discussed herein have also been pointed out by the: Ministry of Community Development, Gender and Children (MCDGC, 2012), Ministry of Education and Vocational Training and Tanzania Law Marriage Act (Parliament, 1971).

   (a) Female Genital Mutilation (FGM)

   Female genital mutilation or female circumcision is a ritual removal of some or all external parts of the female genitalia for non-medical reasons. FGM is often performed with unsterilised razor blades or knives and can lead to bleeding, infections, and childbirth complications. Since complications are common, either during, immediately after the procedure or during childbirth, its victims

are often rushed to district or regional hospitals for medical attention. For any FGM case admission, the police needs to be informed as female genitalia cutting is illegal in the country.

(b) Gender Based Violence (GBV)

Similar to many African countries, Gender Based Violence is also common in Tanzania. The most recent demographic and health survey found that forty four percent of married women in Tanzania have experienced either physical or sexual violence from an intimate partner in their lifetime. While GBV may result in unjustifiable consequences among girls and women; yet these practices are culturally engrained traditions (National Bureau of Statistics, 2011). Similar to FGM, any gender based violence requires police intervention before any treatment from the hospital or other help-seeking channels.

(c) Abortions

With abortion being illegal in Tanzania, most women tend to abort pregnancies themselves or often turn to backstreet clinics run by unskilled providers. It is estimated that about forty six percent of women in urban and sixty percent in rural Tanzania opt for unsafe abortions (MoHSW, 2008b). In addition to severe complications associated with unsafe abortions, the majority of the women who escape death are then transferred from non-registered health facilities to hospitals for immediate medical care.

2. **Ministry of Home Affairs, Police Force**

There are several health-related contexts reported by the Ministry of Home Affairs (MoHA). On the country's crime report for the 2010, the MoHA identified the following:

(a) Non-Surgical Amputation of Limbs

In the past seven years, Tanzania has witnessed an increase in the number of

deaths in people with albinism as well as the number of people with albinism seeking treatment in public health facilities as a result of non-surgical limb amputations. All this began when a rumour spread in some parts of the country that children born without skin pigmentation are imbued with a special sort of magic. Some witch doctors say if you hack off their arms, steal their blood, or even take their lives, riches or luck will come your way. This belief has, in fact, led to the murders of dozens of persons with albinism. Those who escape death may lose a limb and be doomed to live the rest of their lives with disability. Up to the writing of this thesis, the MoHA reported about 60 cases of non-surgical amputations and deaths of people with albinism since 2007.

(b) Throwing Away of Newborn Babies

In Tanzania, throwing away of newborn babies is quite common. From Ministry of Home Affair's crime report, there were 186 cases in 2010 of newborn babies who were thrown away by their mothers for a number of reasons. This is an increase of 8.1% from 172 cases in 2009. In the North Eastern part of the country, majority of the women pointed out some of reasons that led to their decision to throw away their newborn babies, including pressure from their prospective fathers that they do not resemble the newborns as well as an end of a relationship between parents. Usually, when found, these babies are reported to the police force and then taken to the healthcare facilities for treatment and care.

(c) Rape

For the year 2012, Tanzania recorded about 828 rape cases across the country. This is an increase of 48 cases, from 780 cases reported in 2011 (NBS, 2013). Like amputation of albinos, there are some suggestions that the acts of rape, sodomising (104 cases in 2011 and 113 cases in 2012) and child abuse (19 cases

in 2011 and 12 cases in 2012) are also influenced by witch doctors who claim to make people rich if they fulfil their conditions.

(d) House Burning

Healthcare facilities in Tanzania also treat patients who had fallen victims of burning down houses or arson cases. As reported in a crime report by Ministry of Home Affairs, Police Force division, there were a total of 2471 cases in 2012. This is an increase of about 4% from 2375 cases reported in 2011. Majority of these cases are reported from pastoralist communities, and are influences by either theft of the livestock or fighting for land.

(e) Narcotic Drug Use

Tanzania has been used as a transit route for narcotic drugs for abuse between Asia, Middle East and Europe. In recent years, there has been a high traffic of narcotic drugs passing airports and ports, and has resulted into a significant increase in the number of narcotic drug users in the country. Those who have been affected by narcotic drugs usually receive treatment from special units of government-owned hospitals or specialised hospitals (as discussed in Chapter 2).

(f) Vigilantes

The Tanzania Police Force is characterised by a high ratio between police officers and citizens (about 1 police officer is expected to serve 1,294 citizens). Due to this scarcity, as a country, Tanzania has a high number of offenders who commit offences without being caught or prosecuted due to a corrupt judicial system. The frustrations with the judicial system has caused citizens to take measures in their own hands against offenders by either beating, burning or even killing them. The offenders who escape death are usually taken to government-owned hospitals for treatment, under the escort of police officers.

(g) Road Accidents

Since motorcycles began to be used as a mode of commercial transportation, the MoHA registered 11,438 road accidents and 431 deaths. These road accidents result from speeding, negligent drivers, using cellphones while driving, corrupt traffic police and failure to respect and obey traffic regulations (Ministry of Home Affairs, 2012). Majority of individuals injured from road accidents are treated at the Muhimbili Orthopaedic Institute (MOI), which is within the Muhimbili National Hospital (MNH) as well as other government-owned hospitals.

(h) Armed Robbery

The Ministry of Home Affairs recorded 1,332 cases of armed robbery in 2010, which is a 5.5% less than 1,430 cases in 2009. Similar to other cases, victims of armed robberies seek treatment either in public or private health facilities.

(i) Robberies

Unlike armed robberies, there is a high number of un-armed robberies in the country. For the year 2010, there were 6,598 reported robberies in Tanzania, which is an increase of about 10.6% from 7,381 cases in 2009. Additionally, for the year 2011, 6,577 robberies were reported. The majority of the victims of this type of robbery mainly suffers from cuts since knives and swords are commonly used.

(j) Clashes

i. Between Farmers and Pastoralists

For several decades, some parts of the country have observed recurring conflicts between farmers and pastoralists. It is common for these two groups to fight for fertile land, since farmers need land to cultivate crops, and pastoralists require the same piece of fertile land to feed their an-

imals. In addition to claiming lives of innocent people (mostly women and children), these conflicts also result in to more burden for healthcare professionals as those injured will require medical attention.

ii. Between Pastoralist Groups

Between 2010 and 2011, more than 80,000 livestock were reported to be stolen from pastoralists. The majority of those involved with livestock stealing were fellow pastoralists. Similar to clashes with farmers, the clashes between pastoralist groups result into violence whereas a group with stolen livestock usually hunt for those who stole their livestock, and if found, violence erupts. In the overall process of livestock recovery, machetes are used and casualties tend to seek treatment from healthcare facilities without police involvement.

iii. Clashes of the Clans

Pastoralist communities are also involved with clashes between clans as a result of a revenge from either livestock theft or slashing of crops. As arrows, machetes and other traditional weapons are commonly used during these fights, those injured always seek treatment in a nearby health care facility.

3. **Tanzania People's Defense Force (TPDF)**

There are situations that are directly or indirectly handled by the Tanzania People's Defense Force, including

(a) Clashes between Political Parties

For the past ten years, the Tanzania's political scene has been marred with fatal clashes between political parties, forcing military intervention. These clashes have resulted in the deaths of dozens of people and leaving others severely injured and require hospital treatments.

(b) Explosions

In the past two decades, Tanzania has experienced several bomb explosions. The police force has reported numerous home-made bomb explosions in Zanzibar as a result of religious tensions between Zanzibar Muslims and Tanzania mainland Christians. In Tanzania mainland, however, almost all explosions have occurred in army barracks, and thus affecting surrounding citizens. Casualties from these explosions are usually treated in district, regional or military-based hospitals, and the treatments are free.

4. **Ministry of Health and Social Welfare**

The public healthcare facilities in Tanzania offer their services to the residences of the United Republic of Tanzania, depending on different situations:

(a) Unidentified Person and Heath Facility

If there is an unconscious individual being spotted in a public area, citizens of the United Republic of Tanzania are commanded to report such a person to the police force. It is common for those in a general public who are unaware of this requirement to make a decision to take such an unconscious individual directly to the health care facilities without involving the police force. In this case, a patient will receive necessary emergency treatment(s) that the healthcare professional sees fit and the healthcare facility is obliged to report such an individual to the police force. The payment for such treatment will be issued to the patient later.

(b) Payment Type

Since healthcare services in public healthcare facilities in Tanzania are not for free, when a patient visits a healthcare facility, a responsible staff is required to evaluate whether treatment for such a patient is free or not. Among those who receives free treatment in government-owned healthcare facilities are pregnant

women, people suffering from chronic diseases and children under five years of age. In addition to cash payments, another form of acceptable payment is through medical cards.

(c) Police Form Three (PF3)

If there is a medical situation that requires police involvement, public hospitals under the Ministry of Health and Social Welfare (MoHSW) have to check on whether such a patient was supposed to be referred by the police force or not. If the referral is by the police force, either a police officer would accompany a patient to the healthcare facility or a patient has a Police Form 3 (PF3) from the Police Station. If PF3 is missing, patient would receive emergency treatment (as a healthcare professional sees fit) and a healthcare facility would direct the patient to the police station to report the situation.

Table 4.5 summarises health-related contexts extracted from the Tanzania healthcare system. Although payment and Police Form Three (PF3) have been discussed as contexts on their own rights, in this thesis, they are considered as second level of contexts (column 2 and 3, Table 4.5), which means they can be applied on first level contexts (column 1, Table 4.5). Consider how a victim of rape, which is a first level context, is handled upon arriving to the healthcare facility in Tanzania. Normally, upon arrival to the healthcare facility, a responsible staff is expected to evaluate whether the patient has reported to the police force and thus has a PF3 form or not. With this example, contexts can, therefore, be grouped into levels. More health-related contexts from the Tanzania healthcare system are in Appendix D. Section 4.2.4 presents a summary of organisational rules listed by system administrators in the Tanzania's healthcare system.

Table 4.5: The health-related contexts from the Tanzania healthcare system (Source: Author)

Health-related Contexts	**PF3** [Yes or No]	**Payment** [Yes or No]
1. Female Genital Mutilation		
2. Gender Based Violence		
3. Unsafe Abortion		
4. Amputation of Albino		
5. Throwing away of Newborns		
6. Rape		
7. Burning Down Houses		
8. Narcotic Drug Use		
9. Citizen Against Offenders		
10. Road Accidents		
11. Armed Robbery		
12. Robberies		
Clashes between • 13. Farmers and Pastoralists • 14. Between Pastoralists • 15. Clans • 16. Political Parties		
17. Explosions		
18. Unidentified Person		

4.2.4 Organisational Rules from Tanzania Healthcare System

In addition to legislative rules, privacy and security capabilities from national e-health initiatives and contexts (including health-related contexts from the Tanzania healthcare system presented in Table 4.5), the proposed COIL methodology also comprises of internal organisational rules established by the healthcare facilities to govern procedures and operations. The following rules were collected from system administrators working in ten healthcare institutions in Tanzania

O.1 Medical doctors do not need to sign confidentiality agreement with patients as they are bounded by the healthcare professionals' code of conduct (also known as Hippocratic oath which states "Whatsoever I shall see or hear in the course of my dealings with men, if it be what should not be published abroad, I will

never divulge, holding such things to be holy secrets" (Anderson, 1996)).

O.2 A system administrator is allowed to delete medical information of the patient. This access right is, however, restricted since legislation require medical records to be retained for a certain period of time after the patient has left the healthcare facility or die. Most legislation state that, no one is allowed to delete the medical records of the patient until the appropriate data has expired.

O.3 A surgeon consultant is allowed to view theatre schedules and make appointment for his or her patients. A surgeon consultant is also allowed to read patient laboratory results, send laboratory requests and access Picture Archiving and Communication System (PACS) images of the patient.

O.4 A medical doctor is allowed to access medical information of his or her patients. A medical doctor can add and append to it entries to his or her patients' medical records.

O.5 A medical doctor can add private notes about a patient. On the basis of patient-doctor confidentiality which is guided by the Hippocratic oath, these notes can only be accessed by respective doctors.

O.6 Medical doctors are allowed to read patients' laboratory results, radiology images and send patients' laboratory requests.

O.7 A medical doctor is allowed to order prescription if a patient is inpatient and the location where request was generated is a clinic area.

O.8 A nurse is only allowed to view diagnosis of inpatients under his or her care. A nurse is not allowed to view diagnosis of outpatients while visiting a clinic.

O.9 A registered nurse is allowed to view the diagnosis of an inpatient if a nurse is located in the same hospital unit as the patient. That is, a paediatric nurse is

allowed to view medical records of patients receiving treatments in paediatric ward.

O.10 Radiologists are allowed to view information of their respective patients based on their level of work and assigned privileges.

O.11 Pharmacists are allowed to view prescriptions, to access pharmacy store databases as well as to check pharmaceutical stock.

O.12 Registered pharmacists are allowed to view the pharmacy database as well as stock information based on the grants provided at their levels.

O.13 A system administrator cannot add medical entries to healthcare information system of the hospital. A system administrator can, however, set-up and maintain user accounts, maintain system and monitor performance of the system, among others.

O.14 A system administrator cannot view private notes written by doctors for their patients, and also they cannot sign legal agreement on behalf of patients.

O.15 A system administrator is allowed to add a new patient to the system and start or update the care plan of the patient. This is only possible after consultation with the patient or the patient's representative (as permitted by law).

O.16 To address the scarcity of healthcare professionals in the Tanzania's healthcare sector, it is common to find professionals providing healthcare services to patients with whom they do not have a doctor-patient relationship. This access rule is supported in this thesis by extending role based access control with contexts and obligations to allow healthcare professionals to bypass access rules in an accountable manner.

Based on the examination of legislation, national electronic health initiatives, contexts and organisational rules, this chapter aims to develop a new methodology for gathering comprehensive access control requirements for the healthcare domain, named COIL. The COIL methodology, is discussed in Section 4.3, and includes four main elements, i. contexts (as discussed in Section 4.2.3) ii. organisational rules (in Section 4.2.4) iii. e-health initiatives (in Section 4.2.2) and, iv. legislative rules (in Section 4.2.1).

4.3 The COIL Methodology

To devise comprehensive access control requirements that are appropriate in a Tanzania healthcare system, this research began by examining legislation and national e-health initiatives from selected countries, including United Kingdom, Singapore, Australia and Tanzania. This research also extracted specific contexts from the Tanzania healthcare system and also gathered access rules from its healthcare organisations. The specifications from these four parts were then combined to develop a new methodology for gathering access control requirements named COIL (that is, Contexts,

Table 4.6: The components of the new COIL methodology (Source: Author)

CONTEXTS

1. Subject Contexts
2. Object Contexts
3. Environment Contexts
    - Location
    - Time
4. Health-related Contexts
    - Female Genital Mutilation
    - Gender Based Violence
    - Abortion
    - Non-Surgical Amputation of Limbs on People with Albinism
    - Throwing away of Newborns
    - Raping
    - House Burning
    - Narcotic Drug Use
    - Vigilantes
    - Road Accidents
    - Armed Robbery
    - Clashes between Farmers and Pastoralists
    - Clashes between Between Pastoralists
    - Clashes between Clans
    - Clashes between Political Parties
    - Explosions
    - Unidentified Person

ORGANISATIONAL RULES

1. A system administrator is allowed to delete medical information of the patient. This access right is, however, restricted since legislation require medical records to be retained for a certain period of time after the patient has left the healthcare facility or die. Most legislation state that, no one is allowed to delete the medical records of the patient until the appropriate data has expired.
2. A surgeon consultant is allowed to view theatre schedules and make appointment for his or her patients. A surgeon consultant is also allowed to read patient laboratory results, send laboratory requests and access Picture Archiving and Communication System (PACS) images of the patient.
3. A medical doctor is allowed to access medical information of his or her patients. A medical doctor can add and append to it entries to his or her patients' medical records.
4. Medical doctors are allowed to read patients' laboratory results, radiology images and send patients' laboratory requests.
5. A medical doctor is allowed to order prescription if a patient is inpatient and the location where request was generated is a clinic area.
6. A nurse is only allowed to view diagnosis of inpatients under his or her care. A nurse is not allowed to view diagnosis of outpatient while visiting a clinic.
7. A registered nurse is allowed to view diagnosis of inpatient if a nurse is located in the same hospital unit as the patient. That is, a paediatric nurse is allowed to view medical records of patients receiving treatments in paediatric ward.
10. A system administrator can not add medical entries to the healthcare information system of the hospital. A system administrator can, however, set-up and maintain user accounts, maintain the system and monitor the system performance, among others.
11. A system administrators can not view private notes written by the doctors for their patients, and also they can not sign legal agreement on behalf of patients.

TANZANIA LEGISLATIVE RULES

1. Patients medical data should only be obtained from a data subject (patient).
2. Patients medical data should only be collected and processed by healthcare professionals or individuals who are working on their behalf (known as data processors in the European Directive on Data Protection).
3. The purpose(s) of medical data collection and processing should be defined before any transactions. Any changes in the original purpose should be communicated to a data subject.
4. Healthcare professionals must obtain permission (known as consent) from patient before undertaking any medical procedures. The intended consent can be verbal, non-verbal (such as raising a hand to agree) or in writing, by signing a consent form.
5. An individual patient should be allowed to appoint a representative who will be allowed to access medical data on his or her behalf. The representative should be treated in the same way as an individual whose information is being processed.
6. Every person should be allowed to access their medical data either directly, through a healthcare professional or even through a representative as permitted by law.
7. Patients may request to review and rectify errors concerning their medical data.
8. In any circumstance, correspondence between patient and a healthcare professional should remain private.
9. Access to medical data may be refused, limited or delayed, if restricted by law.
10. There should be policies, legislation and procedures that restrict, control or hamper patients access to information and services via the Internet and other communication media.
11. Appropriate measures (administrative, technical and physical) should be implemented so as to prevent medical information from unauthorised access and modification.
12. To deal with emergency accesses, which are common in healthcare, healthcare providers are required to determine types of emergency situations that would require access to information system or application that contain Electronic Health Records (EHRs).

e-health INITIATIVES

1. User identification and authentication
2. Authorisation (Role-Based Access Control is commonly used in the domain)
3. Emergency Access Procedure
4. Auditing and Alerts
5. Patient Consent

Organisational rules, national e-health Initiatives and Legislation). In case of contexts, health-related contexts were collected as part of a three-month observation survey conducted at the Muhimbili National Hospital, and later verified by official documents from ministries and agencies. The documents from the following ministries and agencies were used: Ministry of Community Development, Gender and Children (MCDGC), Ministry of Health and Social Welfare (MoHSW), Ministry of Home Affairs (MoHA) and Surface and Marine Transport Regulatory Authority (SUMATRA).

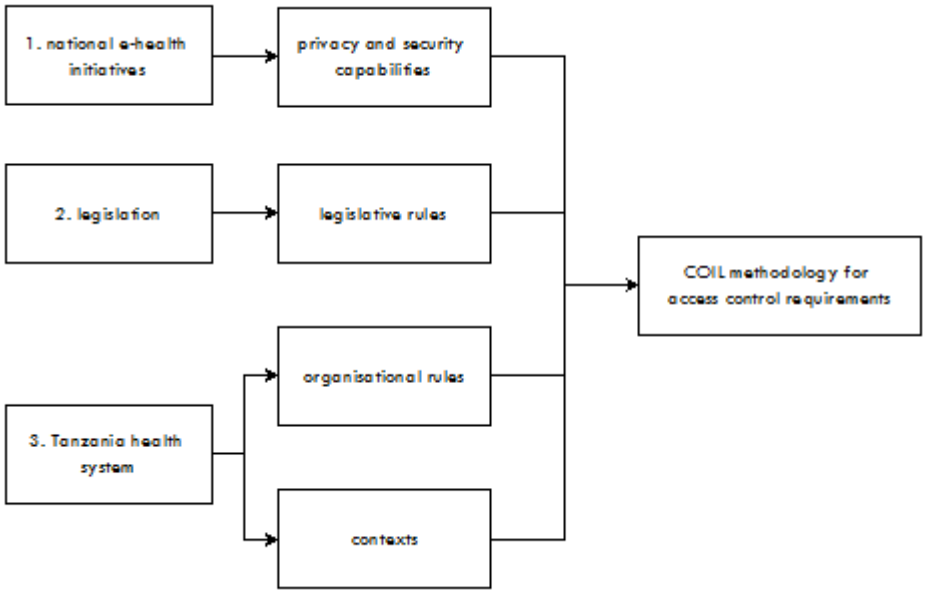


Figure 4.1: COIL: A comprehensive access control requirements in healthcare (Source: Author)

The proposed COIL methodology, presented in Table 4.6 and its components summarised in Figure 4.1, is a result of desk research and observation survey. It comprises of legislative rules, from e-health legislation, and organisational rules that were set out by the surveyed healthcare organisations to govern internal procedures and operations. While contexts results from an observation survey conducted in the year 2012 in the Tanzania healthcare system, the privacy and security capabilities came from an analysis of national e-health initiatives. Based on where elements of these four main

components came from, legislative rules and privacy and security capabilities can be adopted by others conducting research in access control requirements in healthcare, while contexts (particularly, health-related contexts) and organisational rules could be specified based on domain-specific information.

Table 4.7: Gathering access control requirements using COIL methodology (Source: Author)

Component	**Item(s)**	**Yes** [✓], **No** [×]
Contexts		
Privacy and Security Capabilities	User identification and authentication	
	Authorisation	
	Emergency access procedure	
	Auditing and alerts	
Legislative rules		
Organisational rules		

Contrary to the research work by Beznosov (1998) and Alhaqbani & Fidge (2007) where only organisational access rules have been identified and used in to the design of their access control models for the healthcare domain, this thesis presents a new methodological methodology named COIL for gathering comprehensive access control requirements. The COIL methodology supports the continuity of care through enforcement of accountable sharing of electronic health records. The access control requirements discussed in this section can also be used as a guideline to evaluate the design of an access control system (using a check list as shown in Table 4.7).

Table 4.8: Access control requirements for the Tanzania healthcare system, using COIL Methodology

No.	COIL			
	contexts	**privacy and security capabilities**	**legislative rules**	**organisational rules**
1.	×	✓	×	✓
2.	✓	✓	✓	✓
3.	✓	✓	✓	✓
4.	✓	×	✓	✓
5.	✓	✓	×	✓
6.	✓	✓	×	✓
7.	✓	×	×	✓
8.	×	✓	✓	–
9.	×	×	✓	✓
10.	×	✓	✓	✓

To test the validity of the four elements of the proposed COIL methodology, system administrators (labelled with numbers 1 to 10 in Table 4.8) from ten distinct hospitals in Tanzania were asked to evaluate the proposed methodology by choosing either a tick or an x in what they considered as either appropriate or inappropriate category for access control requirements in the healthcare domain. As shown in a summary of results of its evaluation presented in Table 4.8, organisational rules was selected by most of the respondents (90 percent). While 70 percent of the respondents indicated privacy and security capabilities from national e-health initiatives as more relevant, 60 percent selected contexts. Furthermore, 60 percent of the respondents selected legislative rules.

4.4 Conclusions

This chapter has discussed the development of a new methodology, named COIL, for gathering comprehensive access control requirements for the healthcare domain. The newly developed COIL methodology is a combination of four different areas of

research that might affect access to electronic health records. These include: contexts, privacy and security capabilities, legislation as well as rules that govern procedures and operation within the healthcare organisation. The chapter began with an analysis of legislation from United States of America, Europe and, at last, Tanzania that have been designed to control access to electronic healthcare information. From this first set of the review, it was found out that Tanzania is in a process of establishing three cyber security laws (that is, Data Protection and Piracy Act, Computer Crime and Cybercrime, and Electronic Transactions) that will strengthen electronic healthcare adoption and create a foundation for specific electronic healthcare regulations in the country.

Further investigation on national electronic health initiatives yielded several privacy and security capabilities purposely proposed to control access to electronic healthcare information. These are user identification and authentication, authorisation (especially, Role-Based Access Control (RBAC) model which has been widely adopted and used in the domain), an implementation of functions for emergency access procedure, auditing and alerts together with patient consent. To test its validity and to show how the developed COIL methodology could be used, the chapter also contains results of the evaluation of the proposed methodology. From the list of privacy and security capabilities addressed in this chapter, Chapter 5 develops a new context-based access control model, called Role and Context-Based Access Control (RoC-BAC) which supports the continuity of care through enforcement of an accountable sharing of medical records.

Chapter 5

The RoC-BAC Model

This chapter presents a new access control model called Role and Context-Based Access Control (RoC-BAC), which enables access to patient information in the healthcare domain with consideration of changes in contexts. The proposed model is an extension of the traditional Role-Based Access Control model with contexts and obligations, and thus it provides fine grained and flexible access for both frequent and infrequent access requests. The rest of this chapter is organised as follows. Section 5.1 introduces the chapter. Section 5.2 presents the new RoC-BAC model, where its components and relations are discussed followed by its formal definition using mathematical notations. Section 5.3 presents a descriptive example of how RoC-BAC can be used in a Tanzania healthcare system and Section 5.4 concludes the chapter.

5.1 Introduction

Many access decisions in critical emergency systems are usually influenced by individual characteristics and choices. The highly dynamic nature of some environments has, however, introduced new challenges to protected resources. Privacy and security is one of the main issues in critical emergency systems as sensitive information can be accessed or acquired without proper authorisation. As pointed out in Chapter 1, Section 1.3.2 , the main aim of this thesis is to design a new context-based access control model that allows healthcare workers to bypass access rules in an accountable manner in case of unexpected (emergency) situation. The proposed RoC-BAC model is an extension of the conventional, policy-neutral, Role-Based Access Control (RBAC) model with contexts and obligations. In addition to being fine-grained, RoC-BAC model is dynamic, flexible and scalable and incorporates procedures for emergency access requests.

The reason behind a decision to incorporate health-related contexts into RBAC lies on accumulating evidence available on the existing literature. Many researchers in Ubiquitous Computing, where context has been thoroughly studied, point out that, when context is appropriately incorporated into an existing access control solution, the resulting model may improve security in critical applications. Consider the significance of context in a military base as an example of improvement in security. Normally in a military base, a user is allowed to fire a missile if that user is assigned a certain role (for example, a top secret commander) and a user is in a specific high security location at a certain time only. Consequently, a missile can be fired only when it is in a certain location at a certain time. By adding location and temporal constraints in access decision, additional verification checks are henceforth included that must be satisfied before an individual user is granted access to fire a missile.

Break-The-Glass (BTG) procedure is a significant approach for extending access privileges for a user who does not have access to certain information so as to gain access when necessary (Brucker & Petritsch, 2009). The procedure draws its name from breaking the glass to activate a fire alarm. The healthcare systems that contains primary source data (information) for treatment must therefore develop, document, implement and test BTG procedures that would be used in the event when healthcare professionals require unexpected (emergency) access to those records. These systems must have a clearly stated and widely understood procedure for allowing access using an alternate or manual method. It should be noted that, the usage of emergency access rights facilitated by BTG approach needs to be documented for later audits and reviews. As discussed by National Electrical Manufacturers Association *et al.* (2004), examples of infrequent situations that may require BTG and logging could be

i When user experiences account problems such as forgotten username or password or both (after an extended absence or vacation), locked password (as a result of mistyping many times) and even no user account (e.g. a clinician from another organisation or a new clinician is assisting in facility during an emergency)

ii. When there is an authentication problem including failure of the Central Authentication System server, smart card or biometrics reader failure (that is, when a smart card reader or biometric is damaged), and

iii. When there are authorisation problems, including an emergency situation which thrusts an individual user into a role where he or she lacks sufficient access rights (for example, an administrative assistant is entering orders during emergency).

As acclaimed by Ferreira *et al.* (2009), another reason for an implementation of BTG procedure in healthcare is that access control policies are defined with "maximum freedom of access" and "maximum user responsibility" in order to ensure that nothing interferes with the delivery of care. To guarantee maximum freedom of access, infor-

mation systems in healthcare must provide mechanisms for users to access requested information any time, whenever the need arises. With maximum responsibility, systems in healthcare must provide a mechanism that offers additional information such as an alert making users requesting access to be aware that, the user is trying to access unauthorised information under normal healthcare settings or even through a call for help from other qualified people. Abstractly, this makes an individual user requesting such access to information responsible for what user is doing and may subsequently be held accountable. The system must also provide a mechanism that automatically notifies all responsible parties in relation to that access so that user's actions can be justified afterwards.

To address this and other significant access control requirements for the healthcare domain as discussed in Chapter 4, this Chapter discusses a new context-based access control model called Role and Context-Based Access Control (RoC-BAC), that allows healthcare professionals to bypass access rules in an accountable manner in case of unexpected (emergency) requests. With the proposed model, a new concept called health-related contexts is introduced. Section 5.2 discusses a new Role and Context-Based Access Controll (RoC-BAC) model.

5.2 RoC-BAC Model

The Role and Context-Based Access Control (RoC-BAC) model is an extension of the traditional Role-Based Access Control model with the notion of health-related contexts and obligations. The model has been designed to allow healthcare professionals to bypass access rules in an accountable manner in case of unexpected (emergency) requests.

This section is organised as follows: Section 5.2.1 defines components and relations

that make up a RoC-BAC model, and Section 5.2.2 presents operation types in RoC-BAC. Section 5.2.3 presents its formal definition and Section 5.2.4 discusses an augmentation of obligations into the model.

5.2.1 RoC-BAC: Definition of Components and Relations

This section defines components as well as relations in RoC-BAC model. To allow context-based access in healthcare, the RoC-BAC model incorporates health-related contexts in its access decisions so as to allow healthcare professionals to bypass access rules, and hence to support the continuity of care.

RoC-BAC model comprises of the following components:

- Users (U) denote entities requesting access to objects. They may include human beings, processes, machines, networks or autonomous agents. Mathematically, U = $\{ u_1, u_2, \ldots, u_i\}$ denotes a set of users.

- Roles (R) represent organisational job functions with clear definition of inherent responsibility and authority. The concept of roles, as is used in this thesis, is adopted from the RBAC model where users are assigned to roles (user roles) and roles are associated with permissions (permission roles). In RoC-BAC, however, roles represent a combination of user roles (UR) and context roles (CR), as such $R \subseteq 2(UR \times CR)$

- An object (OBJ) is a passive entity that contains or receives information. A set of objects (OBJ) is represented mathematically as, OBJ= $\{obj_1, obj_2, \ldots, obj_j\}$,

- An operation (OPS) is an execution of a program-specific function that is invoked by the user. OPS = $\{ops_1, ops_2, \ldots, ops_k\}$, denotes a set of operations recognised by the system.

- Context (C) is defined as a set of variables that define a situation (Federenko *et al.*, 2004). Contrary to traditional access control models that do not take into account contexts in determining whether access should be allowed or not, RoC-BAC offers a context-centric access control solution, that allow system administrators to define permissions based on the relevant contexts. Mathematically, C = $\{c_1, c_2, \ldots, c_x\}$. For access control purposes, contexts in this thesis are categorised in four groups:

1. Subject Contexts (SC): define contexts that must be exercised by the subject in order to obtain access rights to an object or resource. In RoC-BAC, subject contexts are used to determine access rights for an entity requesting access privileges. They may include the subject's role, identity, credentials, name, organisation that the subject is affiliated with, activity, location, and task (Omary *et al.*, 2011).

2. Object Contexts (OC): An object is a passive entity that is acted upon by a subject. Similar to subjects, objects contain contexts that can be used to control their accesses. Object Contexts (OC) refer any object-related information that can be used to characterise the situation in which the protected object was created and its current status, which is relevant for making an access control decision.

3. Environment Contexts (EC): Environment Contexts describe operational, technical, and even situational contexts at the time a transaction takes place. They may include current date and time, temperature, network's security level, air quality, light level, noise level. These factors are neither associated with a subject nor a resource, but may nevertheless be relevant in controlling access (Omary *et al.*, 2011).

4. Health-related Contexts (HC): define the healthcare domain specific contexts that would be evaluated by an access control system during access decision. From a list provided in Chapter 4, some of the health-related contexts from the Tanzania healthcare system include Gender-Based Violence (GBV), Female Genital Mutilation (FGM), non-surgical amputation of limbs for people with albinism, clashes between: pastoralist groups, pastoralist and farmers, among others. Even though the main aim of this thesis is to extend the traditional RBAC model with health-related contexts; these four groups can further be used to define context roles in RoC-BAC, and thus extending the traditional RBAC model with contexts.

- User Roles (UR) represent a set of user roles. User role is similar to "role" or "subject role" as used in a traditional Role-Based Access Control (RBAC) model.

- Context Roles (CR) describe a set of context roles. It is used to capture relevant contexts that can be used in RoC-BAC policies. In addition to health-related context roles, RoC-BAC also contains time-based context roles, location-based context role and location and time-based context roles, which are part of environment contexts. Typically, $CR \subseteq UR$

- Permission (P) is an approval to perform an operation on one or more objects. Permission (P) $= \{p_1, p_2, \ldots, p_w\}$, is a set of permissions in a system such that $P = 2^{OPS \times OBJ}$. PermOperation: $ops(p : P) \rightarrow \{ops \subseteq OPS\}$, is a permission-to-operation mapping which gives a set of operations associated with a permission p. PermObject: $Obj(p : P) \rightarrow \{obj \subseteq OBJ\}$, a

permission-to-object mapping which gives a set of objects associated with permission p.

- Session (S) represents a set of sessions. Usually, a role is activated for a user during each session. Activated Role (AR) is a mapping between user roles (UR) and Context Roles (CR).

The RoC-BAC model consists of several relations, including User Assignment (UA), Permission Assignment (PA) and Context Role Assignment (CRA). These relations define associations between users, user roles, permission roles and context roles.

- User Assignment (UA): $UA \subseteq U \times R$, a many-to-many mapping that assigns a user role to a user.
- Context Role Assignment (CRA) is a mapping that assigns context to a user role, such that $CRA \subseteq UR \times C$
- Permission Assignment (PA): $PA \subseteq P \times R$, a many-to-many mapping that assigns permissions to a role.
- $assigned\_users(ur : UR) \rightarrow 2^U$, mapping of user role "ur" onto a set of users. Formally: $assigned\_users(ur) = \{ u \in U \mid (u, ur) \in UA\}$
- $assigned\_permissions(r : R) \rightarrow 2^P$, mapping of role "r" onto a set of permissions. Formally: $assigned\_permissions = \{ p \in PRMS \mid (p, r) \in PA\}$
- User Sessions: $user\_sessions(u : U) \rightarrow 2^S$, is a mapping of user u onto a set of sessions.
- Session Roles: $session\_roles\ (s : S) \rightarrow 2^R$, is a mapping of session "s" onto a set of roles. Formally: $session\_roles(s_i) = \{r \in R \mid (user\_sessions(s_i), r) \in UA\}$
- $avail\_session\_perms(s : S) \rightarrow 2^P$, denotes permissions available to a user in a session $= \bigcup_{r \in session\_roles(s)} assigned\_permissions(r)$

5.2.2 RoC-BAC Operations

There are several types of operation that can be performed on RoC-BAC components. Some of the important operation types are presented in Table 5.1.

For the users of the system, three operations (create, update and delete) can be performed during either registration to use the system, profile update and in case of user quitting his or her job as part of the organisation. Similarly, roles can be created,

Table 5.1: RoC-BAC Operation Types

Component	**Operation Types**	**Remarks**
User	create, read, update, delete	These operations can be performed on users of the system either during user registration, profile update or even in case of user quitting
Role	create, read, update, delete	A role is a job function or job title within the organisation. They can be created, read, updated and deleted on request
Location	create, read, update, delete	Location is regarded as part of environment context, and are independent of subjects and objects contexts . Location is, however, associated with both subjects and objects.
Timing	create, read, update, delete	Similar to location, timing is part of environment context where both subjects and objects can be manipulated
Health-related Context	create, read, update, delete	A health-related context is a type of context that allows specification of a health-related reason in an access control policy. Health-related contexts allow healthcare professionals to bypass access rules in an accountable manner thus ensure the continuity of care. They can be created, updated or deleted
Permission	create, read, update, delete	A permission on patient records in a RoC-BAC model can be manipulated using four operations: create, read, update and delete
Session	define, detect, permission right	A session is defined beforehand, permission rights are detected for a session and finally patient information can be obtained and returned

updated or deleted on request. In case of health-related contexts, users of the system are allowed to specify (create) a health-related reason while trying to bypass access rules. These contexts may also be updated or deleted by the system administrator. Contrary to other categories of context, health-related contexts together with obligations help ensure the continuity of care while at the same time enforcing accountability to healthcare professionals.

5.2.3 Formal Definition

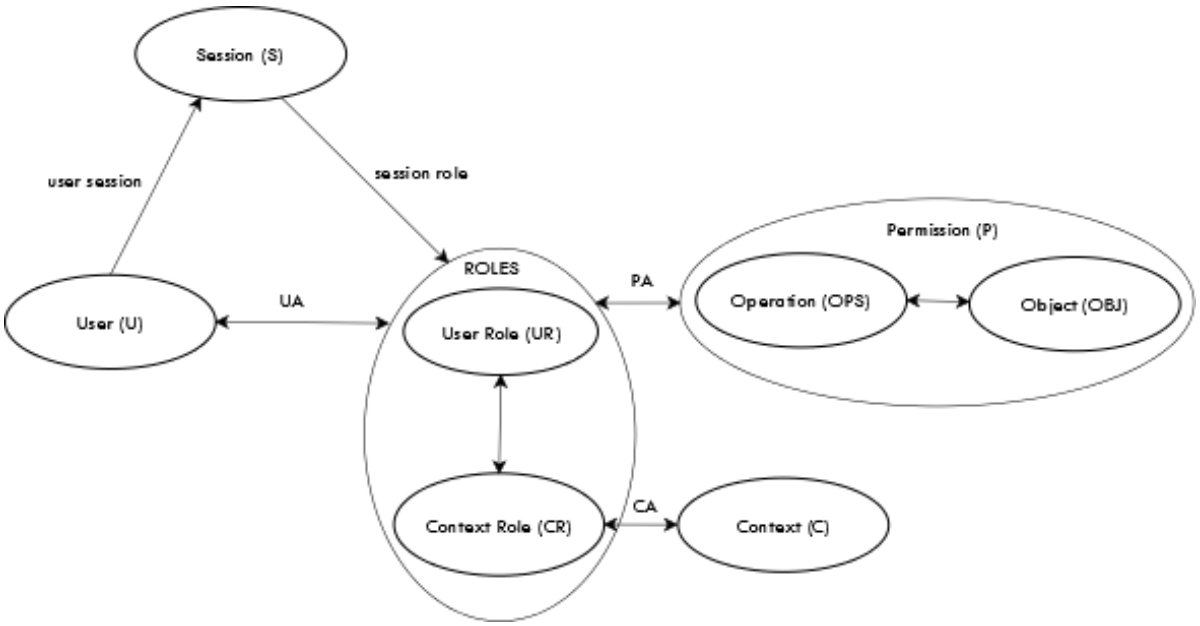


Figure 5.1: RoC-BAC: Role and Context-Based Access Control model (Source: Author)

The RoC-BAC model, shown in Figure 5.1, has the following components:

- U, R, C, UR, CR, OPS, OBJ, P and S (represents users, roles, context, user roles, context roles, operations, objects, permissions and sessions respectively).
- $UA \subseteq U \times R$, many-to-many mapping of user onto user role assignment relation.
- $assigned\_users(ur : UR) \rightarrow 2^U$, the mapping of user role "ur" onto a set of users. Formally: $assigned\_users(ur) = \{\ u \in U \mid (u, ur) \in UA\}$
- $R \subseteq 2(UR \times CR)$, set of roles
- $PA \subseteq P \times R$, many-to-many permission-to-role assignment relation.
- $assigned\_permissions(r : R) \rightarrow 2^P$, mapping of role "r" onto a set of permissions. Formally: $assigned\_permissions = \{\ p \in PRMS \mid (p, r) \in PA\}$
- $user\_sessions(u : U) \rightarrow 2^S$, mapping of user "u" onto a set of sessions.
- $session\_roles\ (s : S) \rightarrow 2^R$, mapping of session "s" onto a set of roles. Formally: $session\_roles(s_i) =$

  $\{r \in R \mid (user\_sessions(s_i), r) \in UA\}$

Definition 1. Context Role (CR) = { L_CR, T_CR, Hr_CR}

CR represents a set of Context Roles. They are used to capture context-relevant information for RoC-BAC access policies. In addition to health-related context roles, which introduced in this thesis through a notion of health-related contexts, RoC-BAC model also supports the specification of location-based context roles (L_CR) and time-based context roles (T_CR). The context roles share similar characteristics with user roles, which are defined in a traditional RBAC model, such as role activation and deactivation.

- **Definition** 1.1. L_CR (Location-based Context Roles)
  Location-based Context Roles L_CR) is a pair (r, l) where r denotes a user role name and l is the current position of a user role.

- **Definition** 1.2. T_CR (Time-based Context Roles)
  Similar to location, Time-based Context Roles is a pair (r, time) where r is a user role name and t is the current time of a user role.

- **Definition** 1.3. Hr_CR (Health-related Context Roles)
  A Health-related Context Role (Hr_CR) is a pair (r, hr) where r is a user role name and hr represents a patient's current health condition which requires healthcare professionals' attention, thus referred as a health-related reason for access.

Definition 2: Authorisations

Location-based authorisations are policies that define accesses that users may have over certain locations. While temporal authorisations limit periods of time during which an authorisation is valid, health-related authorisations define accesses that users may have in case of an unexpected emergency. Formally, they are defined as follows:

- **Definition** 2.1: L-Auth (Location Authorisation)
  A location authorisation is a pair ((s, r), l) where
  - s denotes a subject who requests authorisation
  - l is a location
  - r is a role that subject s can be assigned when in location l

  A location authorisation ((s, r), l) means that subject s is authorised to gain role r when in location l. ((Anne, Nurse), Ward) denotes that Anne has a role Nurse when she is in a hospital ward.

- **Definition** 2.2: Ti_Auth (Temporal Authorisation)
  A temporal authorisation is a quadruple ((s, r), t ($(t_s^i, t_e^i]$, $(t_s^o, t_e^o]$), n) where

- Time interval [t_s^i, t_e^i] is an entry duration during which a subject can gain role r to access object o
- Time interval [t_s^o,t_e^o] denotes an exit duration during which a subject s will revoke a role, such that $t_s^o \geq t_s^i$ and $t_e^o \geq t_e^i$
- n is the number of accesses that a subject can exercise $n \in [1, \infty)$

A temporal authorisation ((Anne, Nurse), (8, 17], (17, 8], 50) means Anne is allowed to activate role Nurse between (8:00, 17:00) and a role will be revoked fifty times during (17:00, 8:00) interval.

- **Definition** 2.3: LoT_Auth (Spatial Temporal Authorisation)

  RoC-BAC also specifies spatial temporal authorisation where policies contain both location and time-related information. A spatial temporal authorisation is defined as ((s, r), ops, obj, t ((t_s^i, t_e^i], (t_s^o,t_e^o]), l) where
  - s, r, ops and obj represent subject, role, operation and object respectively
  - l is a location

  A spatial temporal authorisation ((s, r), ops, obj, ftime, etime, l) semantically means a subject s with role r can perform operation ops on object obj under temporal condition ftime and etime and location condition l.

- **Definition** 2.4: Hr_Auth (Health-related Authorisations)

  A health-related authorisation is a pair ((s, r), hr) where
  - s represents a subject who requests an authorisation and
  - r represents a role which s can activate
  - hr is a health-related context that subject s can specify to access records of the patient

  A health-related authorisation ((Anne, Nurse), FGM) means Anne has a role Nurse but can also activate contextual role FGM when there is a new case to be attended in a respective health facility.

Definition 3: RoC-BACA (RoC-BAC Authorisation)

RoC-BAC authorisation is defined as RoC-BACA (Hr_Auth (L_Auth (T_Auth))) where

- L_Auth denotes location authorisation
- T_Auth denotes temporal authorisation
- Hr_Auth denotes health-related authorisation.

Definition 4: RoC-BAC Authorisation rule

The RoC-BAC authorisation rule is defined by the tetrad (s, R_Auth, obj, m)

- s denotes a subject (user) requesting access
- R_Auth is a RoC-BAC authorisation
- obj is an authorised object
- m represents an access mode which can either be read or write.

Using the formal definition of Role and Context-Based Access Control (RoC-BAC) model presented in this Section; to allow easy understanding of the model, a descriptive example on how RoC-BAC can be used is presented in Section 5.3. Section 5.2.4 discusses an augmentation of obligations in RoC-BAC model.

5.2.4 Augmenting Obligations

One limitation of traditional access control mechanisms is their inability to provide users with obligations as a result of executing permitted action. This major weakness may result in the compromise of integrity or security of the system as system integrity, for instance, requires that certain actions performed in a system should always be followed by other action(s) within a limited time frame (Minsky & Lockman, 1985). The RoC-BAC model is, therefore, augmented with obligations that are often imposed by either operational rules, modern corporation regulations or privacy laws. Obligations specify actions that must be fulfilled in conjunction with an authorisation decision (permit or deny) when an access rule is triggered to maintain accountability. Figure 5.2 presents a RoC-BAC model augmented with obligations in order to maintain accountability in the system.

The following four enhancements has been applied to the formal RoC-BAC model

1. A new basic element called OBGS representing a set of valid obligations is introduced. In this thesis, obligation is defined as tasks that must be fulfilled by the system, and they are associated with permissions allocated to roles. They are categorised as pre-obligations, post-obligations, conditional obligations or

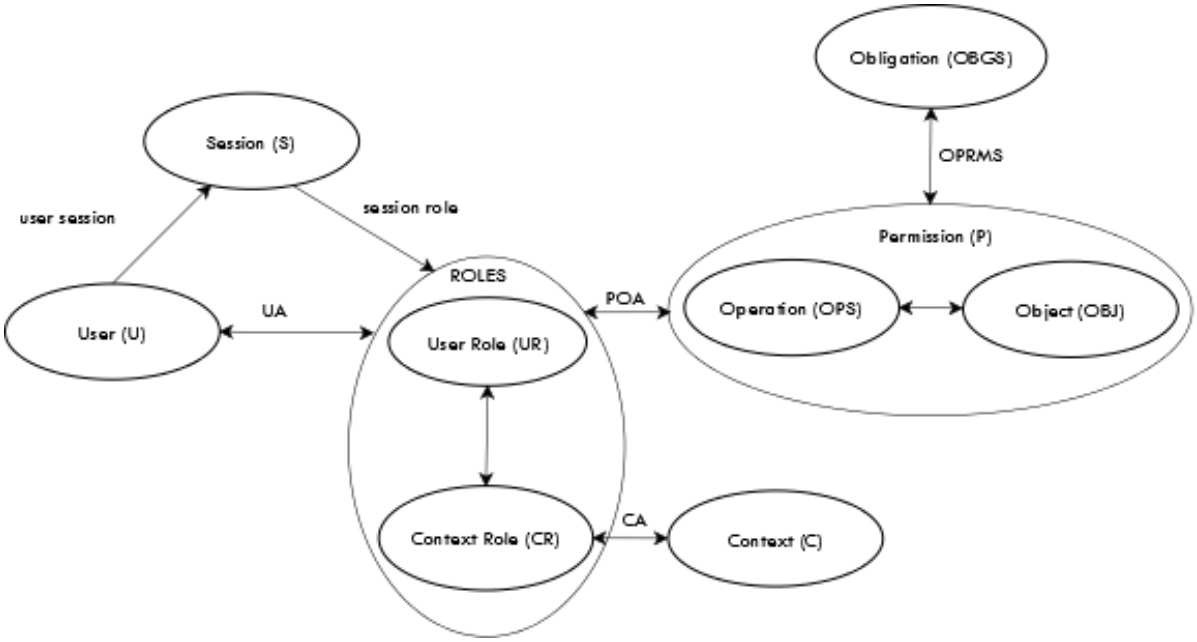


Figure 5.2: An augumentation of RoC-BAC model with obligations

repeating obligations. In this regard, the RoC-BAC model is augmented with post-obligations so as to allow healthcare professionals to access medical records in time, and thus ensure the continuity of care.

2. A new relation called Obligation Permission (OPRMS) is introduced. It represents a relation between permissions (P) and obligations (OBGS), such that $OPRMS \subseteq P \times 2^{\mathrm{OBG}}$. For $oprms = (prms, obgs) \in OPRMS$, means $oprm$ is an obligation augmented permission which specifies if permission prm is exercised, a set of obligations *obg* should be fulfilled.

3. Permission Assignment (PA) relation is modified and a new relation called Permission-Obligation Assignment (POA) is defined. Formally, $POA \subseteq ROLES \times OPRMS$. For $p = (r, oprms) \in PA$, it means role r is allocated with obligation augmented permission $oprm$.

4. To retrieve obligations with authorisation decisions, CheckAccess function is

modified into (Zhao *et al.*, 2007)

$$CheckAccess : SESSIONS, OPS, OBJ \rightarrow BOOL \times 2^{\mathrm{OBG}}$$

The possible combination between authorisation elements and results from Check-Access function are as follows:

- (FALSE, ϕ) $\rightarrow$ DENY access to a resource
- (FALSE,2^{OBG}) $\rightarrow$ DENY access to a resource AND perform obligations on DENY
- (TRUE, ϕ) $\rightarrow$ GRANT access to a resource
- (TRUE, 2^{OBG}) $\rightarrow$ GRANT access to a resource and perform obligations on GRANT

5.3 Use Case

Using the formal definition of the RoC-BAC model presented Section 5.2.3 (summarised in Figure 5.1), a descriptive example of its usage in a Tanzania healthcare system is discussed herein. This descriptive use case is written in order to allow an easy understanding of the model, and how it can be used in case of an infrequent access request.

1. Taking into consideration that an electronic healthcare information system used in this example processes patient information, and for each patient, the system stores three fields: name, age and Blood Group (BG) type. Mathematically, each patient is presented as
   Patient(Name, Age, Blood Group (BG))
2. Components:
   - *Users (U)* = {*Anne, Bob, John*}
   - *Contexts (C)* = { *Location (L), Time (T), Health-related (Hr)* } *C* = { *L*={*Operating Room (OR), Ward, Intensive Care Unit (ICU)*}, *T*= {*Day, Evening, Night* }, *Hr*= {*Ebola, Explosion, FGM, GBV*} }

     Since healthcare is a 24-hour service in almost every aspect, time is therefore divided into three intervals to allow allocation of shifts to healthcare professionals. These are: day shift (from 8:00 a.m to 2:00 p.m), evening shift (from 2:01 p.m. to 10:00 p.m) and a night shift (from 10:01 p.m to 7:59 a.m.). These intervals specify different times a role can be activated. That is, different roles in the same time interval would own different access rights, and the same role in different time intervals would be authorised different

access rights.

- *In RoC-BAC, a role is associated with contexts, and thus, role is a combination of user roles and context roles. Mathematically,* $R = \{UR \cup CR\}$
- *User Role (UR) = {Nurse, Clinical Assistant (CA), Doctor}*
- *Context (C) = {Operating Room (OR), Intensive Care Unit (ICU), Ebola, Explosion, Female Genital Mutilation (FGM)}*
- *Context Role (CR) = {(OR, Nurse), (ICU, Nurse), (Ebola, Nurse), (Explosion, Nurse), (FGM, Nurse), (OR, CA), (ICU, CA), (Ebola, CA), (Explosion, CA), (FGM, CA), (OR, Doctor), (ICU, Doctor), (Ebola, Doctor), (Explosion, Doctor), (FGM, Doctor)}*
- *R = {Nurse, Clinical Assistant (CA), Doctor, (OR, Nurse), (ICU, Nurse), (Ebola, Nurse), (Explosion, Nurse), (FGM, Nurse), (OR, CA), (ICU, CA), (Ebola, CA), (Explosion, CA), (FGM, CA), (OR, Doctor), (ICU, Doctor), (Ebola, Doctor), (Explosion, Doctor), (FGM, Doctor)}*
- *Operation (OPS) = {read, update}*
- *Object (OBJ) = {Name, Age, Blood Group (BG)}*
- *Permission (P)= {read-Name, read-Age, read-BG, update-Name, update-Age, update-BG}*
- *Session =* $\{s_1\}$

3. Session Assignment
   - *user (*s_1*) = {Anne}*
   - *session role = {(Ebola, Nurse)}*
4. Other Assignments
   - *User Assignment (UA) = {Anne, (Ebola, Nurse)}*
   - *Permission Assignment (PA) = {(read-Name, Nurse), (read-Age, Nurse), (read-Blood Group, Doctor)}*
   - *Context Role Assignment (CRA) = {(FGM, Nurse), (FGM, Doctor), (GBV, Nurse), (Explosion, Nurse), (Ebola, Nurse)}*
5. Assignment Process

   Step 1: Role of the User: From Anne's role, Nurse, a set of permission rights to access patient information are identified

   Step 2: Specification of Context: If the user needs further roles that are associated with context, a new window is displayed requesting the user to specify Context (referred as reasons for access in a Context- Enhanced Access in a Tanzania Healthcare (CEATH) system).

   Step 3: When context is specified, the system checks on whether that user is allowed to activate such a context role in that object.

5.4 Conclusions

Information systems that assure accountable sharing of personal information are required in numerous domains, ranging from academic institutions, medical treatment, air traffic control to disaster situations. Privacy and security in these domains depend not only on user discretion or a role that user plays within an organisation, but also on variables that define a situation (referred in this thesis as contexts). This chapter has discussed a new context-based access control model, called Role and Context-Based Access Control (RoC-BAC). The RoC-BAC model is an extension of the conventional RBAC model with health-related contexts and obligations, and has been designed to allow healthcare professionals to bypass access rules in an accountable manner so as to ensure the continuity of care.

To address the inability of traditional access control mechanisms to provide users of the system with obligations as a result of an execution of permitted action, RoC-BAC model is further augmented with obligations where new elements and relations are introduced. Particularly, a new basic element called obligations that represents action(s) that must be fulfilled in conjunction with an authorisation decision is introduced, together with a new relation called obligation permissions that represents a relation between permissions and obligations. For easy understanding of the proposed model, a descriptive example of its usage in a Tanzania healthcare system was discussed in Section 5.3. Chapter 6 discusses prototype implementation of RoC-BAC and RBAC models.

Chapter 6

Implementation of a Prototype

This chapter discusses an implementation of a prototype, named CEATH (Context-Enhanced Access in a Tanzania Healthcare system), which implements the RoC-BAC model. Although RoC-BAC model has already been explained and formally defined in Chapter 5, this chapter addresses it in terms of technical software requirements aimed at developing its prototype. The rest of this chapter is organised as follows. Section 6.1 introduces the chapter with a thorough review on CEATH's objective and research methods. Section 6.2 discusses its architecture followed by data design models in Section 6.3. Section 6.4 discusses CEATH's implementation. The conclusion of the chapter in Section 6.5.

6.1 Introduction

This first section of the chapter presents the realisation of Role and Context-Based Access Control (RoC-BAC) model in terms of prototype implementation. As discussed in Chapter 5, the proposed RoC-BAC model is an extension of the traditional Role-Based Access Control (RBAC) model with the notion of health-related contexts. Particularly, health-related contexts are integrated into the traditional Role-Based Access Control model to allow healthcare professionals to bypass access rules in an accountable manner in case of infrequent access requests so as to ensure the continuity of care. The prototype discussed in this chapter was implemented to demonstrate the applicability of RoC-BAC model and also to measure overheads in execution time introduced by different relations and assignments.

Objectives

As pointed in Chapter 1, in this thesis, a prototype has been implemented in order to achieve two main objectives. These are:

- To experiment and verify that the proposed RoC-BAC model is practical
- To evaluate overheads introduced in execution time by different relations and assignments

Software Methodology

In this research, two software development methodologies were adopted for the implementation of Context-Enhanced Access in a Tanzania Healthcare (CEATH) system. These are: incremental software development methodology, which involves an implementation of a prototype divided into small sections so as to make manageable

changes required during the development process, and prototyping. Since acceptance of any information system depends on the involvement of its users during the software development process, a prototyping method was then adopted for its implementation.Healthcare professionals from selected healthcare facilities in Tanzania, both private and public, were involved during the requirements gathering stage. The following steps were carried out in an incremental software development methodology:

- Requirements gathering,
- Analysis and design,
- Implementation,
- Testing,
- Deployment, and
- Evaluation

In addition to the researcher's competency in using incremental software development methodology in system development, the nature of this work also makes it more promising for the chosen methodology.

To address challenges as well as deficiencies identified in a Tanzania healthcare system that affect the continuity of care, the following generic research methods were employed in this study:

- Interviews with healthcare professionals and system administrators at the Muhimbili National Hospital (MNH) to gain an understanding of how electronic healthcare systems are deployed and used in Tanzania. This part of the research work also involved a survey questionnaire to identify current electronic healthcare systems implemented in Tanzania mainland together with their access control mechanisms. These methods were discussed in Chapter 2.

- A review of literature on best practices concerning access control for different domains (including healthcare), as discussed in Chapter 3.
- Analysis of selected legislative and national e-health initiative documents which are relevant in terms of controlling access to EHRs. Among others, this investigation included an analysis of legislative documents from Europe, United States of America (USA) and Tanzania. The review also covered national e-health initiatives from United Kingdom, Singapore, Australia and Tanzania. This analysis is in Chapter 4.
- Revision and experimentation of open-source EHR systems with the purpose of gaining an in-depth understanding of what the CEATH system should be like, what it should do, and how it should perform. Chapter 7, therefore, discusses an evaluation of the CEATH system, which implements RoC-BAC model (discussed in Chapter 5), against a EMR-RBAC system that implements Role-Based Access Control model. The CEATH system is based on appropriate access control requirements for the healthcare domain discussed in Chapter 4.

6.2 Architecture of CEATH

In this section an architecture for Context-Enhanced Access in a Tanzania Healthcare (CEATH) system is discussed. This section is divided into two parts: Section 6.2.1 discusses the overall design goals and Section 6.2.2 discusses its architectural components.

6.2.1 Design Goals

The core design goal for CEATH system is to keep its architecture as general as possible and thus to address access control requirements identified in Chapter 4. The

inclusion of authentication and context-based authorisation are the two design goals defined for CEATH architecture design.

1. **Authentication:** Authentication is a prerequisite when designing an information system that tries to establish access to protected resources (Evered & Bögeholz, 2004). To fulfil this requirement, an information system should contain a procedure to verify that a person requesting access to a protected resource is the one who she or he claims to be (Mercuri, 2004). However, despite its significance, it is common for researchers in access control to make an assumption that a proper authentication mechanism is already in place and thus shift their focus to just authorisation. With the design of the CEATH system, a simple authentication system that uses a combination of username and password was implemented in order to authenticate users before accessing protected records.

2. **Context-Based Authorisation:** As pointed out in Chapter 3 and 4 in relation to access control requirements for a healthcare system, such a system should be able to grant or deny access based on available contexts pertaining to the time of request. Since the main aim of this thesis is to design and develop a context-based access control model that allows healthcare professionals to bypass access rules in an accountable manner in case of infrequent (emergency) situations, health-related contexts and obligations were incorporated in to the traditional RBAC model, to make it fine-grained and flexible for dynamic environments. The incorporation of health-related contexts in electronic healthcare system is expected to open up the system and to allow it to cope with infrequent (emergency) health situations. The health-related contexts used in this thesis were extracted from the Tanzania healthcare system, which is used as a case study domain for this research.

   In addition to authentication and context-based authorisation, this research also addresses a number of access requirements that are specific to the healthcare do-

main. These requirements have been identified by researchers in academia and documented in various legislation, as discussed in Chapter 4.

- **Emergency Handling:** The healthcare domain follows the "care comes first principle" where a patient's health needs are to be put first before anything else. With this principle in place, an access control system in a healthcare organisation should be designed in such a way that critical emergency situations are handled by overriding existing access rules. If there is a patient who was injured as a result of a road accident, for instance; the nearest qualified healthcare professional should be able to access the patient's basic electronic medical records and provide appropriate care as seen appropriate. This act should be possible even if it violates Role-Based Access Control (RBAC) or any traditional mechanism implemented.

- **Logging and Alerts:** To keep track of all transactions in the system, all access and access attempts to electronic medical records should be logged. While health-related contexts open up the system, the logging and alerts feature would enforce accountability to healthcare professionals by logging all transactions and alert users with senior roles when a transaction with health-related contexts is specified. In CEATH, logging is accomplished using an alerts module where alerts are sent to either a system administrator or any pre-defined healthcare professional with a senior role on any attempt(s) of healthcare workers to access information beyond their specified rights.

- **Legislation:** To address legal and interoperability issues, an access control system designed for any healthcare domain should comply with statutory and technical standards. The proposed laws in Tanzania (that is, Cyber Crime Laws, which is a combination of Data Protection and Piracy Act, Computer Crime and Cybercrime Act and Electronic Transaction Act), are expected to govern personal

data protection (ITNews, 2013). These Acts, especially the Data Protection and Piracy Act, are expected to be a motivation towards adoption and use of electronic healthcare in Tanzania. The needs identified in these proposed laws in Tanzania are also addressed in the proposed RoC-BAC model, and implemented in the CEATH system.

6.2.2 Architectural Components

An architecture for the CEATH system (shown in Figure 6.1) is divided into three parts, namely:

- Users layer
- Access Control layer and,
- Resources layer

The following is a step by step procedure to access medical records [numbered between 1-11 in Figure 6.1]

1. The user authenticates using a combination of username and password by submitting them in to an authentication system
2. The authentication system sends user identification information to the role manager
3. The role manager sends the respective user's role to the authentication system
4. The authentication system verifies the user's identification information against records stored in an authentication information database
5. After successful authentication, the role manager retrieves the respective user's role from the user/role permissions database

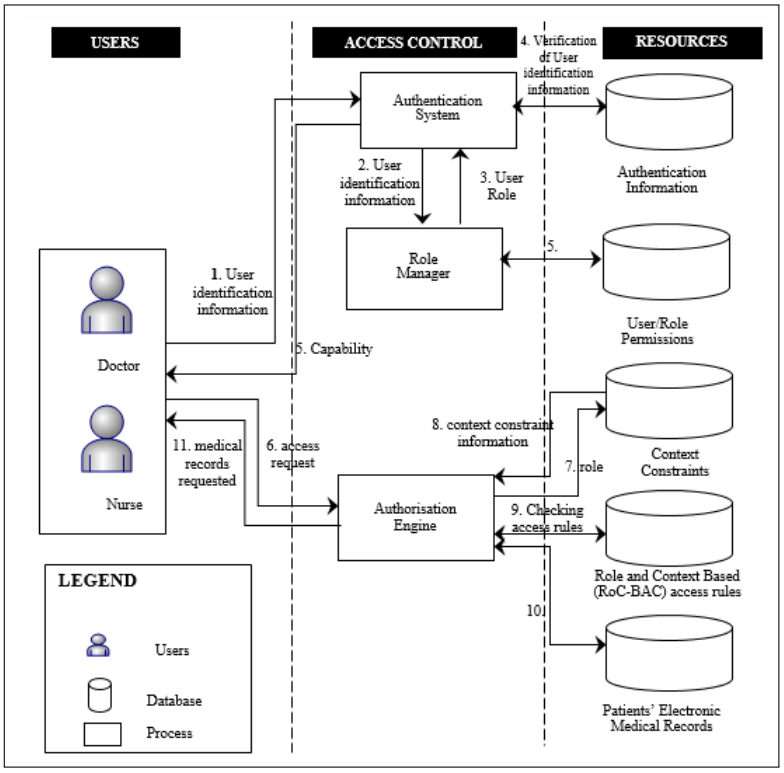


Figure 6.1: A system architecture of the CEATH system (Source: Author)

6. If the user has requested to access medical records, an access request together with the user's role are sent to the authorisation engine

7. The access request is evaluated against a role-based authorisation policy at first, and if such an access is allowed then access is granted. If not,

8. An authorisation engine sends a role to a context constraints database, and

9. Context constraints database sends context constraints information for the role to an authorisation engine

10. An authorisation engine checks access rules in a Role and Context Based access rules database

11. The authorisation engine retrieves requested medical records by requesting them

from patients' electronic medical records database

12. The requested medical records are sent to the user

The main components of the architecture are:

1. **Authentication System:** This system obtains user identification information explicitly by user logging in to a system using provided username and password. The system verifies the information submitted by the user against information stored in an authentication information database, as shown in Figure 6.1. If authentication information is valid, the system then allows an individual user to request access to medical records through an Authorisation Engine. However, if the information provided is wrong, an individual user will be prompted to enter this information again for verification.

2. **Authorisation Engine:** An Authorisation Engine is the core component of CEATH system which controls access to protected medical records. When a user requests access to medical records, an authorisation engine has to perform several tasks before issuing an access decision.

   - At first, an Authorisation Engine obtains an access request and the user's attributes including authentication information for a user who wishes to perform a transaction. It also requests dynamic context attributes associated with such a user, including current location and current time of access, together with context of the resource to be accessed. As shown in the architecture, this is performed against a Context Constraints database

   - An Authorisation Engine then checks with User/Role (also known as authorisation) database for any permissions that were defined for that user. To do so, an authorisation engine checks to see whether the current user is authorised to perform the requested action, by obtaining role and attributes-based

access control rules. The engine then verifies constraints against information in patients' records. The authorisation engine is, henceforth, a component that decides whether to grant or deny users of the system access to protected medical records.

3. **Resources:** The resources layer contains databases that form the core part of any electronic healthcare system. A database is defined as a software program that permits storage and retrieval of information. There are various databases that store different information in CEATH system. These include:

   - **Authentication Information:** As its name suggests, an authentication information database stores users' information used to verify whether the user requesting access to the CEATH system is the one who they claim to be. In fact, when a user requests to use CEATH system, by either creating, updating, reading or editing patient information, an individual user has to submit a combination of pre-assigned username and password, that are verified using information stored in this database. Among others, this database contains user identification, username, password and electronic mail address.

   - **User-Role Permissions:** This database is also referred to as an authorisation database, and it stores all permissible assignments of users to roles or activities in CEATH system. The permissions to a role in a system are usually assigned by the system administrator.

   - **Context Constraints:** This database stores both users' and objects' attributes that must be considered for authorisation purposes. Each context attribute in a database consists of a "key-value" pair, such as "role = nurse". The four groups of contexts specified in RoC-BAC model are subject contexts, object contexts, environment contexts (including location and time) and health-related contexts. Some of the contexts that may be used with RoC-BAC model include

user identification (user ID) that uniquely identifies the user, and is part of subject contexts, role(s) and department to which user belongs which also belong to subject contexts.

- **Role and Context-Based (RoC-BAC) access rules:** This database interacts with an authorisation engine and stores access rules that are primarily used to limit access to sensitive patients' electronic medical records. When an authorisation engine receives an access request from the user, it then requests for all access rules that are appropriate for such a request from Role and Context-Based (RoC-BAC) access rules database. These access rules are administered by the system administrator.

- **Patients' Electronic Medical Records:** This is a database that contains sensitive patients' electronic medical records. In a complete system, this database may include chart notes, laboratory results, medication lists and diagnosis-related information lists. Similar to the RoC-BAC access rules, this database also communicates with an authorisation engine in order to allow the user access to requested medical records.

6.3 Data Design

For an implementation of CEATH, three levels of system design were considered, using models. These are: conceptual, logical and physical (involving the implementation of the data model) model design. Since the complexity of design increases from logical to physical, the design of CEATH began with the conceptual model (shown in Figure 6.2) so as to understand at high level different entities in the system and how they relate to one another.

After a conceptual design, a logical model was designed so as to understand the details

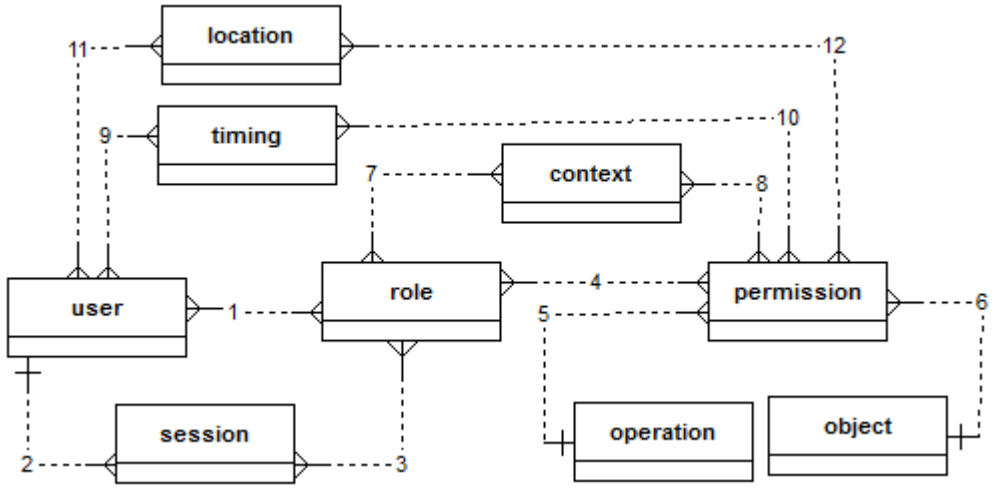


Figure 6.2: A conceptual design model for the CEATH system (Source: Author)

of the data without worrying about how they will actually be implemented (shown in Figure 6.3).

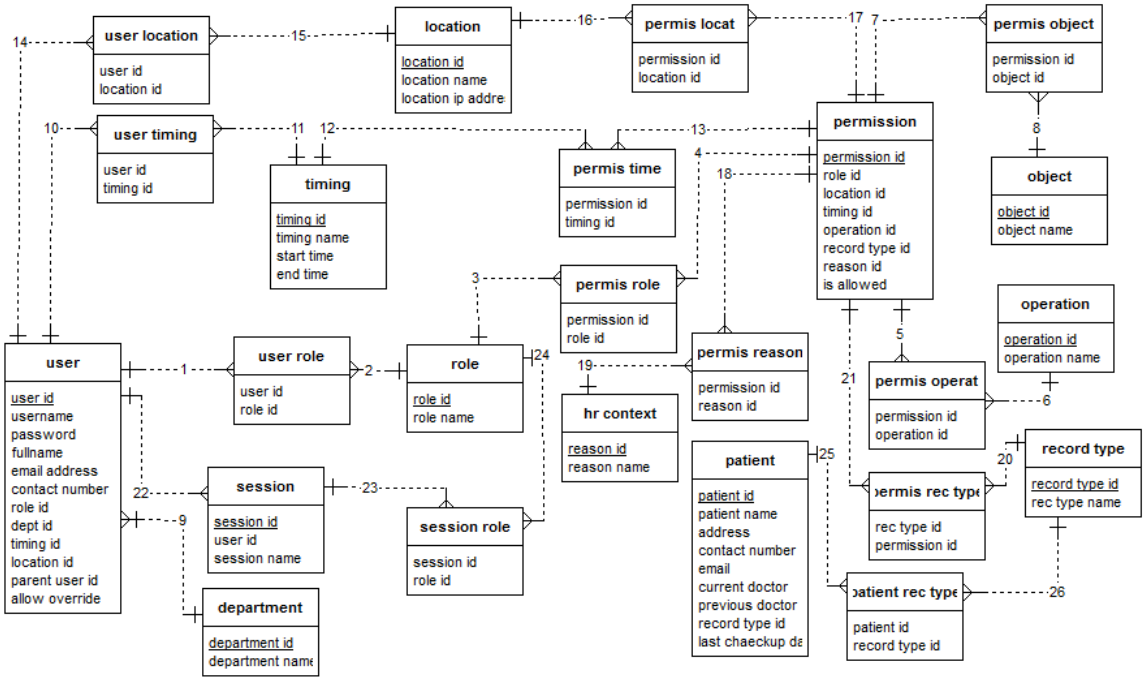


Figure 6.3: A logical design model for the CEATH system (Source: Author)

Its logical model contains twenty four entities and twenty six relations between entities (numbered from 1 to 26). Lastly, a physical model was designed for the implementation of the data model in a database. The entities and business assertions for the physical design model are thoroughly discussed in Section 6.4.

6.4 Implementation

This section discusses the implementation of CEATH system, based on access control requirements defined in Chapter 4 and a proposed context-based RoC-BAC model formalised in Chapter 5.

6.4.1 Business Assertions

The following are business assertions in CEATH system.

Table 6.1: User table (Source: Author)

Field	Type	Null	Key	Default	Extra
user_id	int(5)	NO	PRI	NULL	auto_increment
username	varchar(20)	NO		NULL	
password	varchar(30)	NO		NULL	
full_name	varchar(50)	NO		NULL	
email	varchar(50)	NO		NULL	
contact_no	bigint(15)	NO		NULL	
role_id	int(2)	NO	MUL	NULL	
dept_id	int(2)	NO	MUL	NULL	
timing_id	int(2)	NO	MUL	NULL	
location_id	int(2)	NO	MUL	NULL	
parent_user_id	int(5)	NO		NULL	
allow_override	tinyint(1)	YES		NULL	

1. First and foremost, the system needs to store data about users. For each user,

it needs to store the user's identification (id), username, password, full name (full_name), email address, telephone_number, role identification, user's department, user's shift where a user is allowed to access medical records in a system, user's allocated location and an identification of a senior user (in terms of a role). The value of user identification (user_id) is uniquely used to identify each user, as shown in Table 6.1.

Table 6.2: Department (Source: Author)

Field	Type	Null	Key	Default	Extra
dept_id	int(2)	NO	PRI	NULL	auto_increment
dept_name	varchar(30)	NO	UNI	NULL	

2. Since healthcare professionals work under departments, there is also a need for a system to store information about each department in the healthcare organisation. For each department, dept_id is used to uniquely identify the department, and department name (dept_name), stores the full name of the department, as shown in Table 6.2.

Table 6.3: Role (Source: Author)

Field	Type	Null	Key	Default	Extra
role_id	int(2)	NO	PRI	NULL	auto_increment
role_name	varchar(30)	NO	UNI	NULL	

3. As users are assigned to roles and roles (both user roles and context roles) are associated with permissions, there is a need for a system to store information about each role defined in a system. For each role, there is a role_id which uniquely identifies the role, and role name that stores the name given to a role.

Table 6.4: Location (Source: Author)

Field	Type	Null	Key	Default	Extra
location_id	int(3)	NO	PRI	NULL	auto_increment
location_name	varchar(30)	NO	MUL	NULL	
loc_ip_address	varchar(20)	NO		NULL	

4. To control access within a health care facility using the proposed RoC-BAC model, the system needs to store information about location. This entity is associated with both user and permission. For each location, information stored includes location_id which uniquely identifies the location, location name and assigned ip-address.

Table 6.5: Timing (Source: Author)

Field	Type	Null	Key	Default	Extra
timing_id	int(2)	NO	PRI	NULL	auto_increment
timing_name	varchar(20)	NO	UNI	NULL	
start_time	time	NO		NULL	
end_time	time	NO		NULL	

5. For each timing specified in the CEATH system, the system needs to store unique timing identification (timing_id), timing name (assigned attribute for timing_name), the beginning (start_time) and ending (end_time).

Table 6.6: Operation (Source: Author)

Field	Type	Null	Key	Default	Extra
operation_id	int(2)	NO	PRI	NULL	auto_increment
operation_name	varchar(20)	NO	UNI	NULL	

6. The system is also required to store information about operations supported in the system. For each operation, there is an operation identification (operation_id) which uniquely identifies each operation and an operation_name which stores full name of each operation.

Table 6.7: Record Type (Source: Author)

Field	Type	Null	Key	Default	Extra
record_type_id	int(2)	NO	PRI	NULL	auto_increment
record_type_name	varchar(30)	NO		NULL	

7. There are numerous types of records that can be stored in a single patient's electronic medical record. The system, therefore, needs to store information in relation to different record types. As shown in Table 6.7, a record type in CEATH was defined using two attributes: record_type_id which uniquely identifies the record type and record_type_name to store the name for each record type.

Table 6.8: Reason (Source: Author)

Field	Type	Null	Key	Default	Extra
reason_id	int(2)	NO	PRI	NULL	auto_increment
reason_name	varchar(30)	NO		NULL	

8. To support the continuity of care in an accountable manner, this thesis proposes a new Role and Context-Based Access Control (RoC-BAC) model by extending the traditional Role-Based Access Control (RBAC) model using health-related contexts. To be able to use health-related contexts, the system needs to store information about each health-related context (a reason is used to represent health-related context) as specified by the use. For each reason, there is a reason name (reason_name) which stores the name for each health-related context condition and a reason identification (reason_id) which stores a unique value for each reason.

Table 6.9: Permission (Source: Author)

Field	Type	Null	Key	Default	Extra
permission_id	int(3)	NO	PRI	NULL	auto_increment
role_id	int(3)	NO	MUL	NULL	
location_id	int(3)	NO	MUL	NULL	
timing_id	int(2)	NO	MUL	NULL	
operation_id	int(2)	NO	MUL	NULL	
record_type_id	int(2)	NO		NULL	
reason_id	int(2)	NO		NULL	
is_allowed	tinyint(1)	NO		NULL	

9. For each permission, the system needs to know each and every role requesting access (role_id), location from which access is requested (location_id), time of access (timing_id), operation requested (operation_id), type of record where its access is requested (record_type_id) and health-related context condition through which access is requested (reason_id). Permission identification (permission_id) is used to uniquely identify each permission.

Table 6.10: Notification (Source: Author)

Field	Type	Null	Key	Default	Extra
notify_id	int(5)	NO	PRI	NULL	auto_increment
from_id	int(5)	NO		NULL	
to_id	int(5)	NO		NULL	
record_id	int(5)	NO		NULL	
record_type_id	int(2)	NO		NULL	
reason_id	int(2)	NO		NULL	
other_reason	varchar(50)	YES		NULL	
notify_time	datetime	NO		NULL	
location_id	int(3)	NO	MUL	NULL	

10. For a healthcare professional who has accessed medical records of a patient who is

not assigned access to (for instance when attending an emergency situation), the system needs to be able to notify the user with a senior role (or anyone as assigned in the system) such access in order to enforce accountability. The information stored are presented in Table 6.10, and each notification contains identification of the user who accessed the records (from_id), parent user (to_id) identification of the user where such access is reported, record accessed (record_id), type of record(s) accessed (record_type_id), reason for access (reason_id), time of notification (notify_time) and location of access (location_id). The notify_id is used to uniquely identify each notification.

11. CEATH system was designed from the proposed RoC-BAC model which allows healthcare professionals to bypass access rules in an accountable manner in case of infrequent (emergency) situation. In this thesis, electronic healthcare has been used as a study domain, and thus the system needs to store patients' electronic health records. For each patient, the system needs to store patient name, address, contact telephone number (contact_no), patient's current doctor (curr_doctor_id), patient's previous doctor (prev_doctor_id), record types that are available in patient's electronic health records (identified by the record_type_id), date for patient's last check up (last_checkup_date), as shown in Table 6.11. Each patient is uniquely identified by patient identification number (patient_id).

Table 6.11: Patient (Source: Author)

Field	Type	Null	Key	Default	Extra
patient_id	int(5)	NO	PRI	NULL	auto_increment
patient_name	varchar(50)	NO		NULL	
address	varchar(250)	NO		NULL	
contact_no	bigint(15)	NO		NULL	
email	varchar(50)	YES		NULL	
curr_doctor_id	int(5)	NO	MUL	NULL	
prev_doctor_id	int(5)	YES	MUL	NULL	
record_type_id	int(2)	NO	MUL	NULL	
last_checkup_date	date	YES		NULL	

Considering that CEATH implements Role and Context-Based Access Control (RoC-BAC) model, which is an extension of the traditional Role-Based Access Control (RBAC) model with health-related contexts and obligations, its evaluation involves a comparative performance analysis with a access control system built from a conventional Role-Based Access Control (RBAC) model. As part of its design, Figure 6.4 presents the logical model for the EMR-RBAC model which implements the

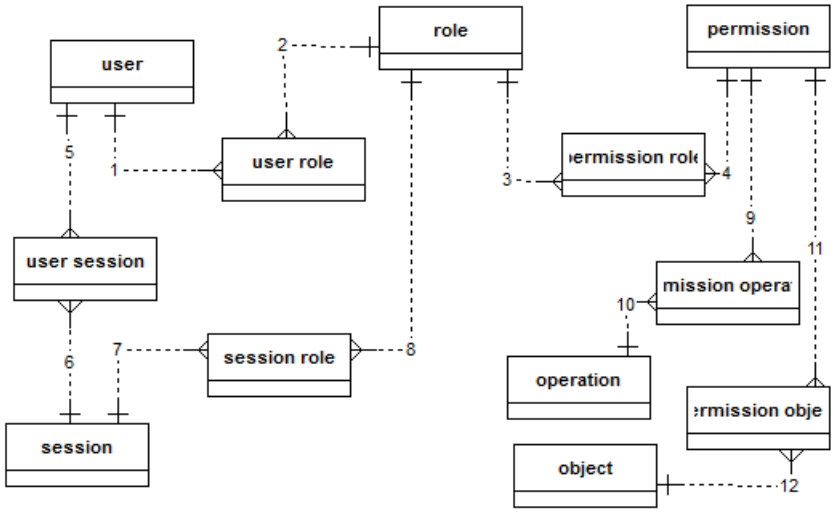


Figure 6.4: Logical model for EMR-RBAC system which implements RBAC model

traditional RBAC model, * indicates a many relationship.

6.4.2 The Prototype

A working prototype was developed using Java as a client side technology and PHP as a server side technology. Some of the steps defined to pursue its development are as follows:

- Creation of a dynamic website prototype with several web pages, including a specific web page for system administrators, healthcare professionals and patients. Access to each these pages is protected by authorisation policies.
- Add a health-related context page that is displayed to healthcare professionals when an initial attempt to access medical records is rejected. The control over who is entitled to specify health-related contexts during an access request is specified in an authorisation policy. After a healthcare professional has successful specified an allowed health-related context from an existing list in the system, patient's medical records should be displayed. The value of a health-related context needs to be passed to an authorisation engine in each access decision, and any such transaction is logged for accountability.
- Add patients electronic medical records in to the chosen MySQL database. The dummy records were created using the dummy patients data obtained from the Muhimbili National Hospital in Tanzania.
- Add a post obligation policy to health-related context operation. When a user with medical doctor role has agreed to access protected records through the specification of health-related context, an obligation should be set and activated whenever user requests to access records that he or she is not normally authorised.
- An evaluation of CEATH system which implements RoC-BAC model against EMR-

RBAC system which implements RBAC model.

6.4.3 Experimental Results

For implementation and evaluation, the two prototypes were deployed in a local server. For the CEATH system, the deployed prototype contained the following:

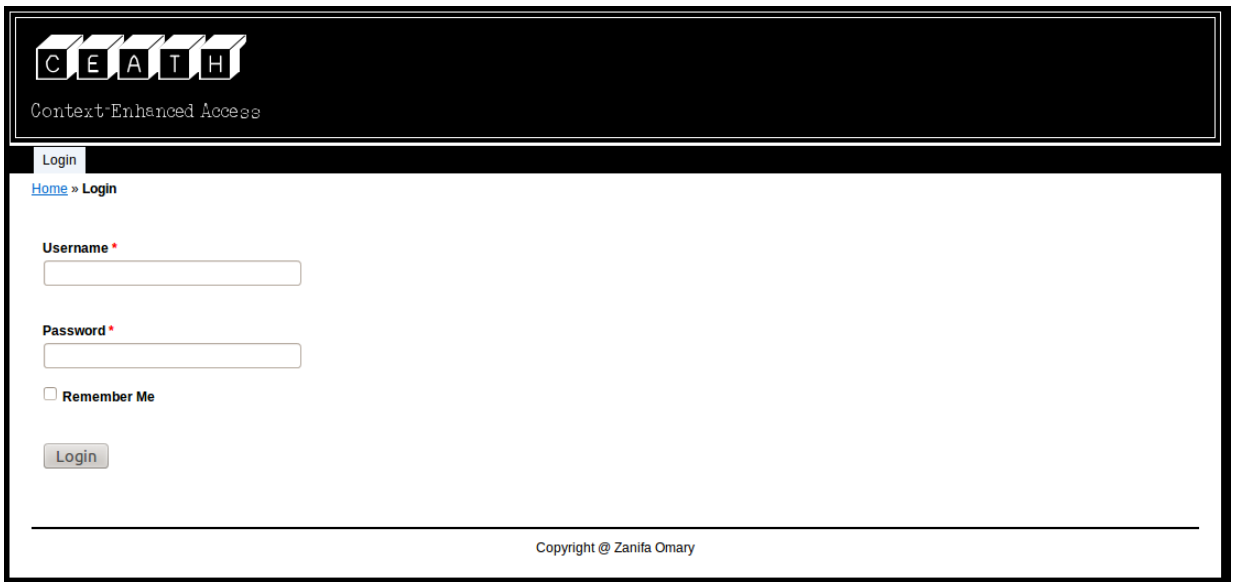


Figure 6.5: Login page of the CEATH System

- The first publicly accessible page allows users to log in to the system. When a user selects the home page button, a login screen shown in Figure 6.5 is presented. Each user of the system needs to authenticate first using a combination of username and password before accessing any records. The valid username, password together with a role associated with each user will trigger an Authorisation Engine to check if such a user can access requested patient records. After successful login, the logged in user is then directed to either system administrator's page (shown in Figure 6.6) or healthcare professionals page.

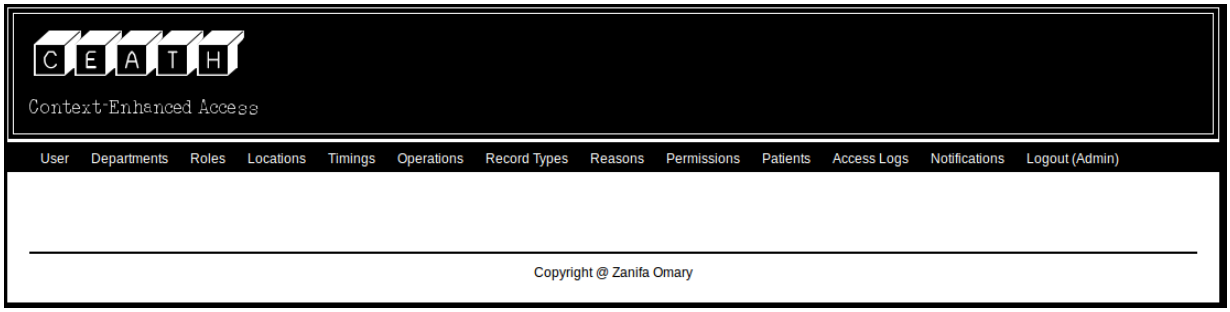


Figure 6.6: System administrator's page in CEATH System

For users who have successfully logged in to the system, they are redirected to their appropriate pages depending on their role category. This can either be system administrator's page, healthcare professional's page or patient's page. Offering patients' access to their health records is out of scope of this thesis, and thus only two pages are shown.

- If a user is restricted to access the requested medical records, a health-related context page is returned. Consider, as an example, when an authenticated user named Linda with a physiotherapist role, based in a physiotherapy department, at the Amana hospital tries to access patient's records from another department. In this scenario, a context specific page, shown in Figure 6.7, will be displayed and the user is required to select a reason behind request to access restricted medical records. If the user is not allowed to access records with specification of health-related context, a rejection page will be returned.

- If a user carries out access by accepting accountability to what he or she has requested to access by specifying a health-related context (named reason), as shown in Figure 6.8, CEATH's Authorisation Engine is then asked to confirm if such a user can specify health-related context on a specified resource. If the answer is GRANT, a set of obligations is returned and a page with confidential

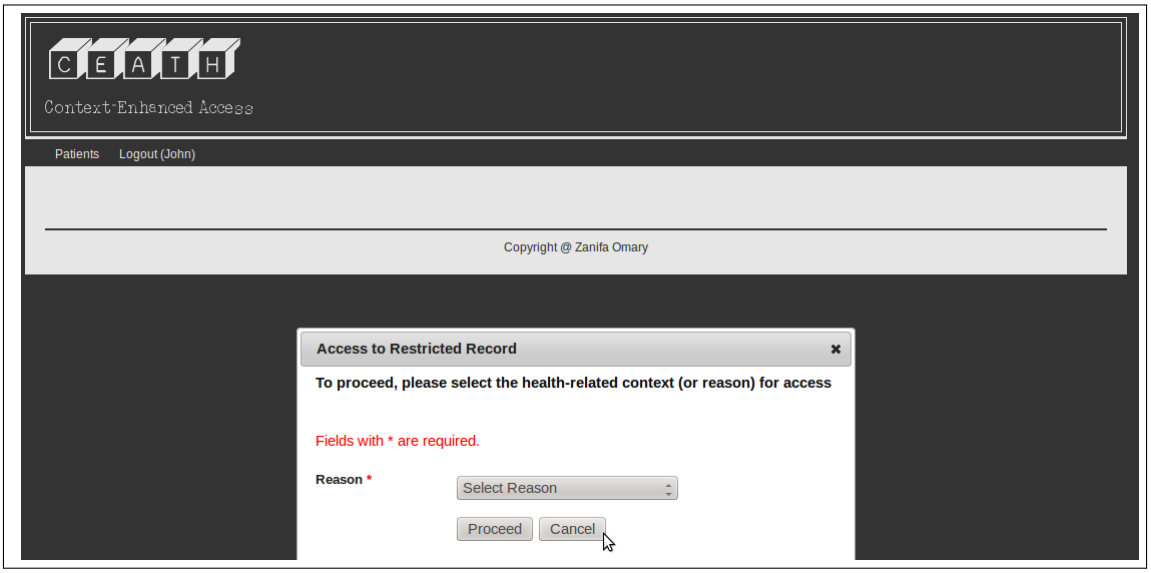


Figure 6.7: Access with health-related context specification

medical records is displayed.

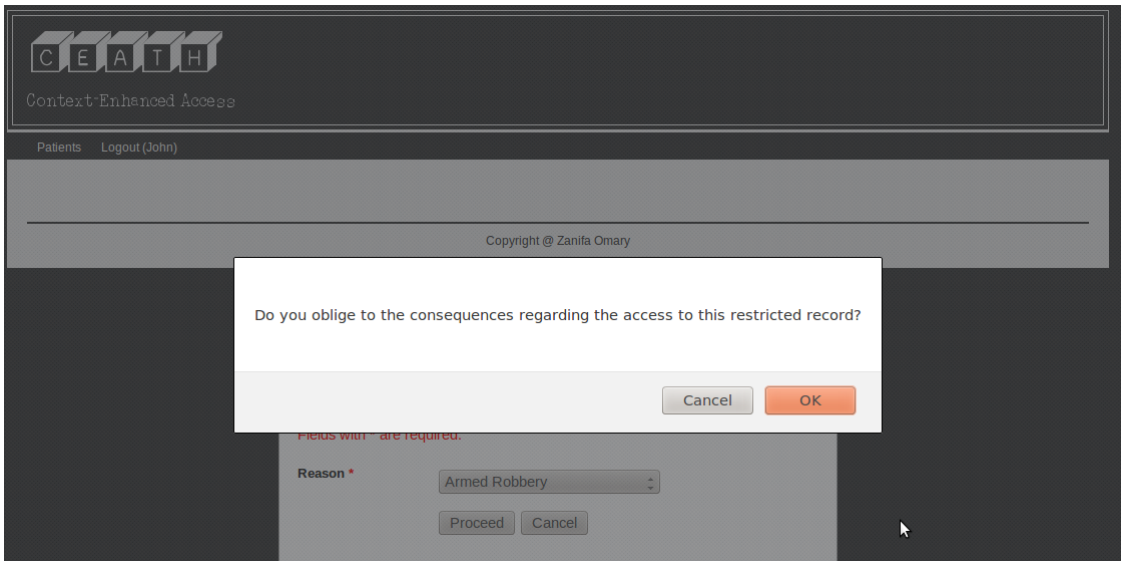


Figure 6.8: Obligation Confirmation

To enforce accountability, CEATH system maintains an access log with information on who has accessed patient records, as shown in Figure 6.9.

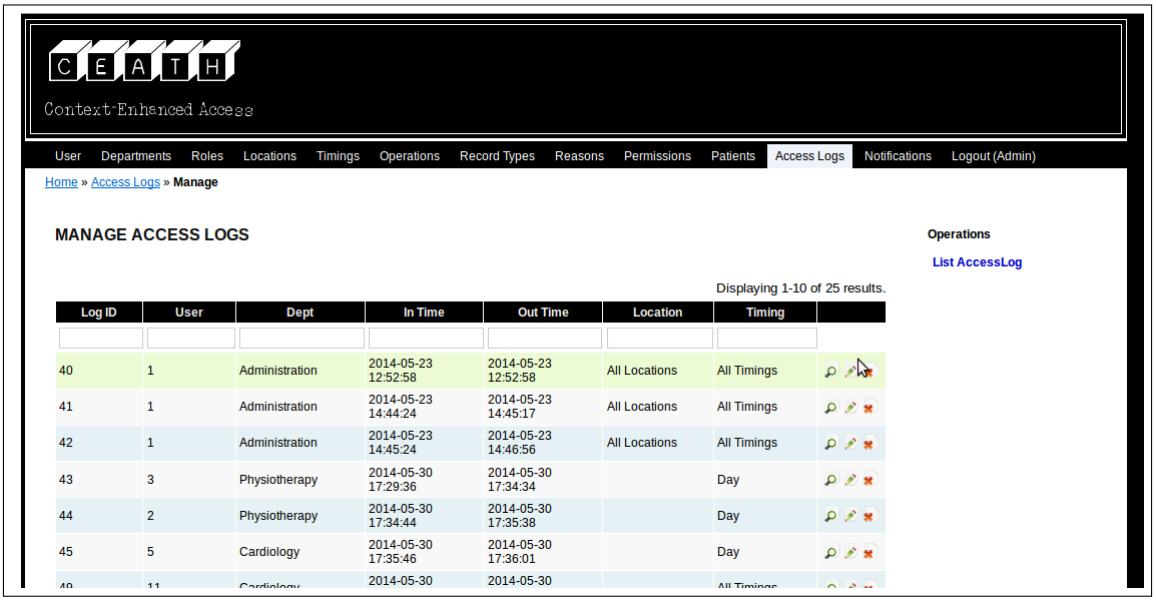


Figure 6.9: Access log from CEATH

To make sure that healthcare professionals and other healthcare workers are held accountable for their decisions to access medical records, it is necessary for notifications to be sent to a senior role when an individual user requests to access protected records through health-related context specification. The number of context specific accesses in the system are logged, and system administrators can then learn from them so as to improve the system and also to reduce the number of infrequent accesses in future by creating and implementing access rules for them. Figure 6.10 presents a notification page from CEATH system.

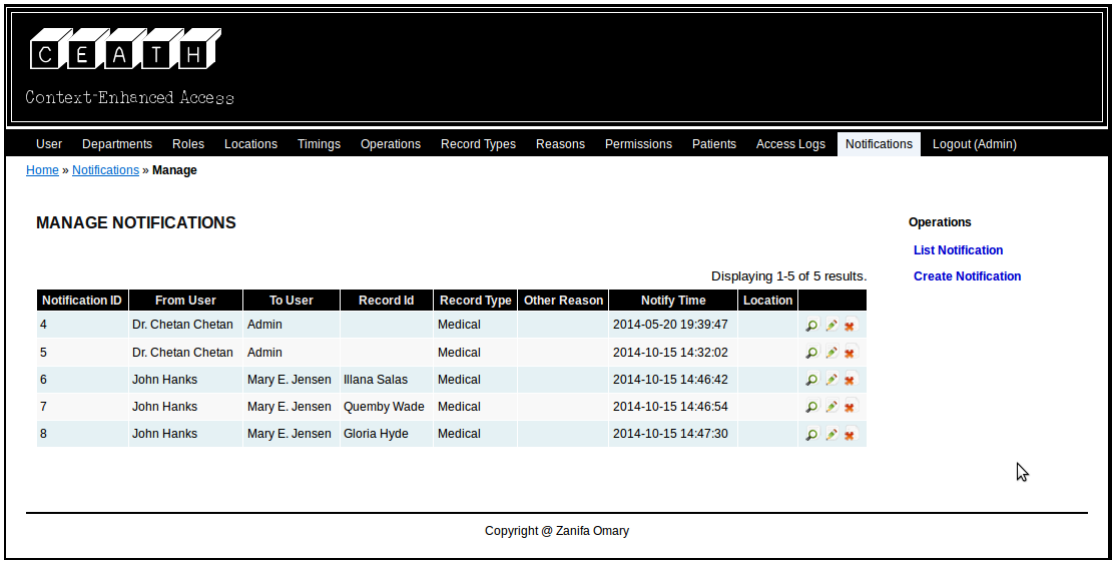


Figure 6.10: Notifications

6.4.4 Health-related Context Variable

Two tables were created and stored in a database to hold information about users of the system and patients' medical records. The users' table holds information about the user including a user's assigned unique id, username, password, contact_no, email, role(s) assigned to a user, department to which user belongs, assigned location, timing as well as a user with a senior role. The patients' table holds information about the patient. This includes patient unique identification, patient name, address, contact number, email, identification of the current and previous doctor(s), type of records in EHR and patient's last check-up date.

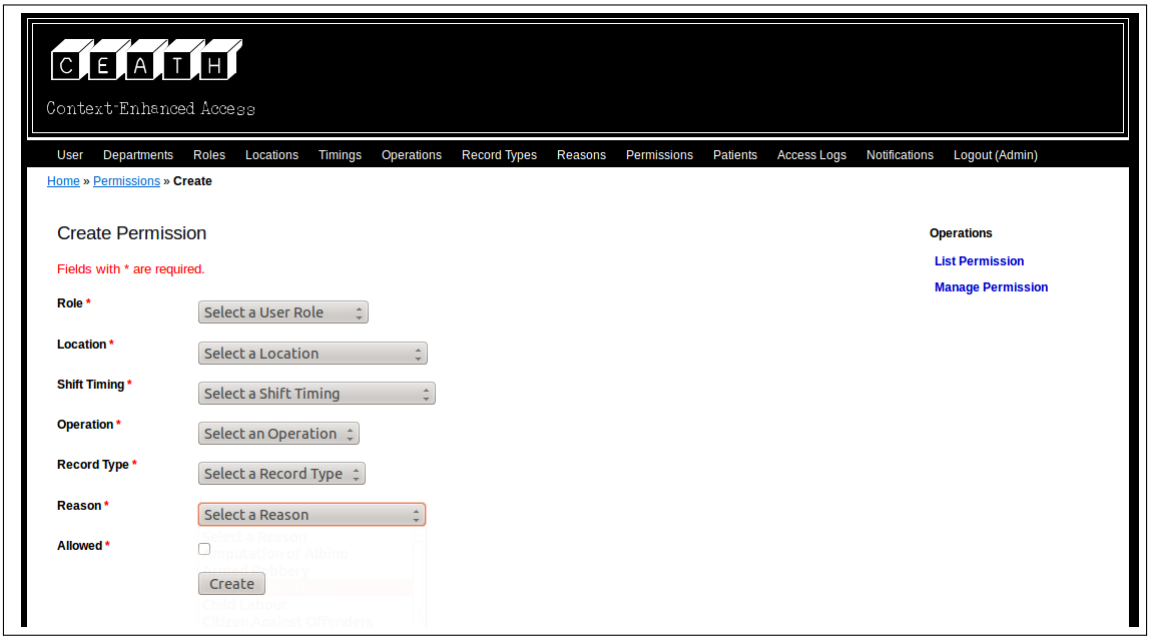


Figure 6.11: Permissions

To allow healthcare professionals to be able to bypass access rules, a context variable named "allowed" was created. This variable has NULL as a default value and can be specified by a system administrator. To be able to set or reset the context boolean variable state for users of the system, an administrative interface was created that allowed a system user with a system administrator role to set or reset the variable manually to either TRUE or FALSE, as shown in Figure 6.11.

6.4.5 EMR-RBAC

To provide complete management of authorisation data in the EMR-RBAC system, which implements Role-Based Access Control (RBAC), Yii's Role-Based Manager (RBAM) was used. RBAM contains an authorisation item (auth item, shown in Figure 6.12), which is a fundamental concept behind the implementation of Role-Based Access Control via a browser interface. Generally, the RBAC model in RBAM is implemented in terms of roles, tasks and operations. A role is a collection of tasks,

operations and other roles. An operation is a single action on an object, and a task is a collection of operations. Through authorisation items, a system administrator in an EMR-RBAC can create a role, a task or an operation.

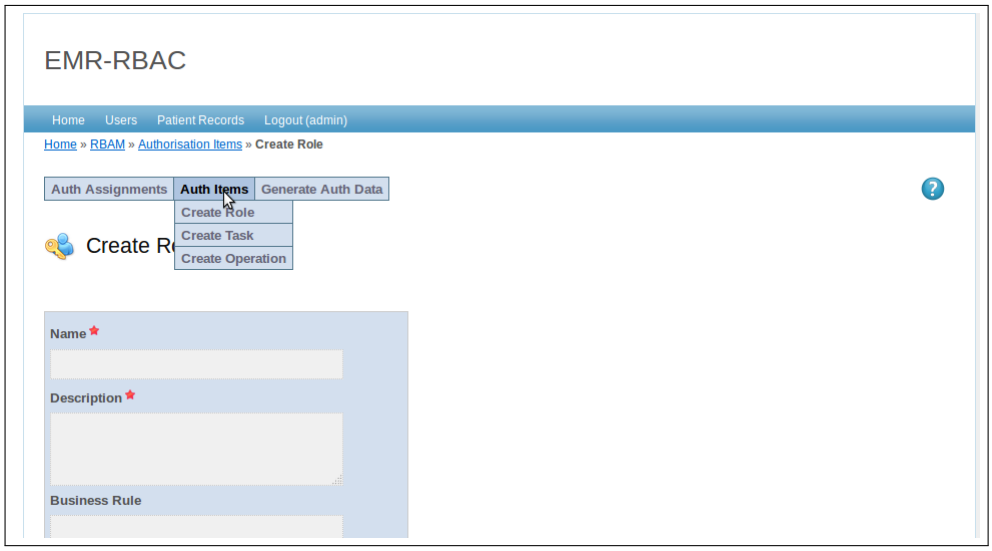


Figure 6.12: Yii's authorisation item

Figure 6.13 shows role assignment page for the EMR-RBAC system through a Role-Based Manager (RBAM) module.

6.5 Conclusions

This chapter has discussed a successful implementation of a prototype for the proposed Role and Context-Based Access Control (RoC-BAC) model. Mainly, the prototype has been implemented in order to demonstrate how the RoC-BAC model can be implemented. Contrary to traditional access control mechanisms which use identity of its users to control access, CEATH evaluates contexts in its access decision to allow healthcare professionals to bypass access rules in an accountable manner in case of an infrequent access so as to support the continuity of care.

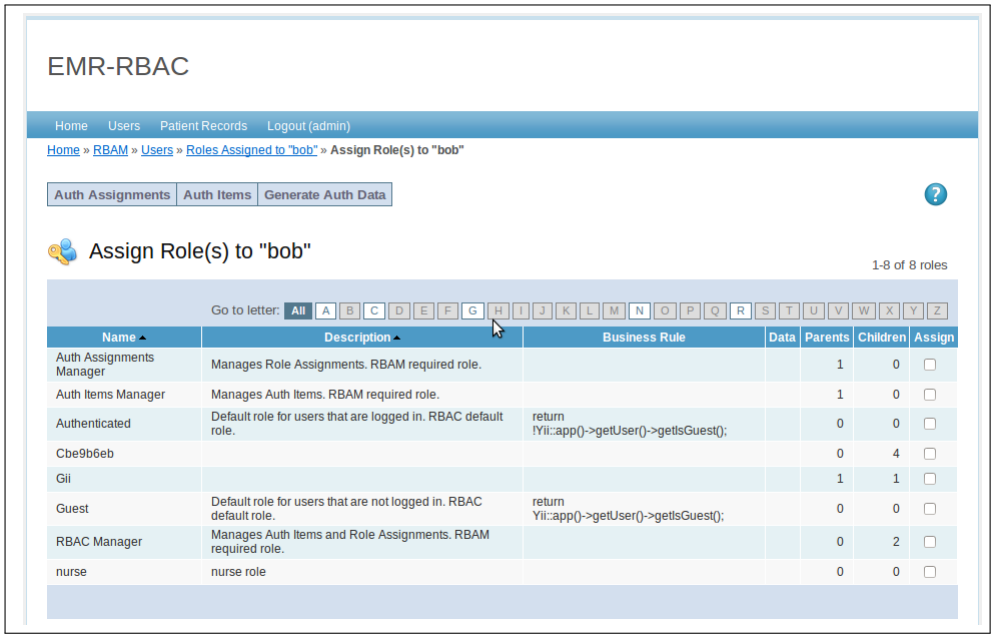


Figure 6.13: Role assignment in EMR-RBAC system

To support this significant principle in healthcare, especially for an environment with limited human resources for health, this thesis extends the traditional Role-Based Access Control (RBAC) model with health-related contexts and obligations. This chapter discusses implementations of two prototypes, named CEATH and EMR-RBAC, which implements RoC-BAC and RBAC models respectively. With the definition of health-related contexts that pertains to contexts associated with specific area of an application, RoC-BAC can henceforth be adopted and used in other domains that suffer from limited human resources. Chapter 7 discusses different aspects of evaluation of RoC-BAC model, which is implemented through the CEATH system.

Chapter 7

Evaluation

This chapter presents the results of an evaluation of the Context-Enhanced Access in a Tanzania Healthcare (CEATH) system, discussed in Chapter 6. The chapter begins with a review of criteria proposed by NIST that can be used to evaluate access control systems in Section 7.1. Section 7.2 examines access control mechanisms, including RoC-BAC, with respect to criteria discussed earlier. Section 7.3 evaluates the effect of various elements and relations in CEATH by comparing its performance against that of a pure RBAC system. Section 7.4 discusses expert user evaluation of the CEATH system. Section 7.5 presents an analysis and discussion followed by the conclusion of the chapter in Section 7.6.

7.1 Evaluation Criteria

In this section, criteria for evaluating access control systems are discussed. These criteria have been proposed by the National Institute of Standards and Technology (NIST) and can be used to evaluate access control systems (Hu *et al.*, 2006), (Hu & Scarfone, 2012). The evaluation criteria discussed include granularity of control, dynamicity, flexibility and adaptability, scalability, user mobility, reliability and performance.

1. Granularity of control

   Granularity is an extent to which a system can be broken down into small parts, either the system itself, its description or observation. It can either refer to the extent to which a larger entity is subdivided, or the extent to which groups of smaller entities have been joined together to become larger distinguishable entities. Granularity is defined as "a relative size, scale, level of detail or depth of penetration that characterises an object or activity" (TechTarget, 2005). As a simple example in measurements, a yard broken into inches has finer granularity than a yard broken into feet.

   There are two levels of granularity when describing an access control system, that is fine-grained and course-grained. While course-grained description of a system is associated with larger subcomponents, a fine-grained description regards smaller subcomponents of which larger ones are composed. Section 4.2.8 of the NIST document (Hu & Scarfone, 2012) explains this characteristic that enables privacy control of the same information with different classification of data fields in a record. In some instances in access control, a fine-grained access does not refer to characteristics of a data object or resource but rather to refer to conditions that apply during access. These may include time of the day, location of access, organisational assignment and clearance level (Axiomatics, 2013). Taking this notion into con-

sideration, the higher the number of contexts allow for finer granularity of access control, and since RoC-BAC was purposely designed for a healthcare domain, and it supports the specification of many contexts as discussed in Chapter 5, this thesis has therefore shown that RoC-BAC is fine-grained.

2. Dynamicity

   The healthcare environment is constantly changing since health care workers are in constant movement,

   As a result of health care workers being in constant movements, the healthcare environment is characterised as being dynamic with constantly changing scenarios. With these characteristics, support for dynamicity is therefore considered as an important feature for any access control mechanism which can be used in an environment that evaluates dynamic context information while making access decisions (Hu *et al.*, 2006). Through its support of the four categories of contexts, the newly proposed RoC-BAC model is considered to support dynamicity.

3. Flexibility and Adaptability

   This criterion is addressed in Section 4.2.10 of the NIST document by Hu & Scarfone (2012). The section contains two questions that could be used to evaluate an access control system. These are:

   - Is the access control system capable of dynamically interposing access control rules based on system states?
   - Is the access control system capable of handling the evolution of the organisation's future access control policy changes?

   Since a typical healthcare system witnesses a large number of varying scenarios and unforeseen events, this criterion is used to evaluate an ability of access control mechanism to adapt to those scenarios and events. To cope with these changes,

an access control mechanism for the healthcare domain should be both flexible and adaptable. Since the main aim of this study was to design a context-based access control model that allows health care workers to bypass access rules in an accountable manner using contexts and obligations, the proposed RoC-BAC is both flexible and adaptable.

4. Scalability

   Scalability is defined as "an ability of a computer application or product (both hardware and software) to continue to function well as it is changed in size or volume to meet user needs" (TechTarget, 2006). A healthcare system crosses the boundary of a single healthcare institution and even that of the healthcare service as a whole. Thus, the number of eventual users of the system and ways of its usage is likely to be unpredictable. Consequently, scalability of an access control mechanism is a significant factor in healthcare.

5. Support for user mobility

   Providing for user mobility in access control will result in an enhanced system that allows high priority users, such as doctors, to access patient data with high priority situations from different places in a healthcare institution, from different institutions and even from home. This criterion will, therefore, enable such users not to be constrained by locations while trying to offer health care services to patients.

6. Reliability

   In a distributed computerised system with a large number of components, the failure of one or more components at any time is inevitable. In a healthcare system which needs to be always available, the access control system should be highly reliable in spite of the failure of components.

7. Emergency Access

For emergency situations, an access control system should allow healthcare professionals to bypass the access policy (access rules). To address this, healthcare providers are required to determine the type of situations that would require access to an information system or application that contain EHRs. Section 4.2.2 of the document by Hu & Scarfone (2012) contains an evaluation item for this criterion: " Is the access control system capable of bypassing access rules for critical access decisions?". The metric for this will either be Yes or No depending on the capability of the system. RoC-BAC was designed to allow health care professionals to bypass access rules in an accountable manner by extending the traditional Role-Based Access Control with contexts and obligations.

8. Performance

   Section 4.3 of the document by Hu & Scarfone (2012) lists four functions that may be considered to evaluate the performance of an access control system, including: response time, policy repository and retrieval, policy distribution and an integration with an authentication function. This thesis considers only two (response time and integration with an authentication function) out of the four criteria to evaluate performance.

   (a) Response time: As discussed in Section 4.3.1 of the document by Hu & Scarfone (2012), three items may be used to evaluate the performance of an access control system in relation to response time. These include:

   - Does the response time of granting an access request meet the organisation's requirement?
   - Does the response time for the maximum number of access requests in an expected time frame meet the organisation's requirement?
   - Does the response time for activating and revoking access rules meet the

organisation's requirements?

However robust an access control mechanism may be, user acceptability of a system depends highly on its response time. With the high volume of data processed, stored and transferred in healthcare systems, special care has to be taken to ensure that the right trade-off between performance and other properties of an access control system.

(b) Authentication function: Section 4.3.4 of the document by Hu & Scarfone (2012) points out this feature with an item that evaluates on whether an access control system is integrated with authentication function or not. Usually, there are different types of users who request access to information in a healthcare system, and thus different authentication mechanisms need to be implemented in order to provide the right type of access to its users. In addition, different authentication mechanisms may be required for different access levels. In CEATH system, a simple authentication system that uses a combination of username and passwords was implemented. Table 7.1 summarises each criterion by incorporating its corresponding item that could be used to evaluate the access control mechanism.

Table 7.1: Evaluation criteria and their associated questions (Source: Author)

Evaluation criteria	**Item(s) to evaluate**
Granularity of control	Does an access control system allow configuration of granularity of controlled objects? The metric for this will either be course-grained (if the mechanism supports single or no context at all) of fine-grained if multiple contexts are supported
Dynamicity	Is the management of authorisation in an access control system static (such as in RBAC, where permissions are administratively associated with roles and users are administratively made members of appropriate roles) or dynamic (where access decision depends on availability of contexts and other factors)?
Flexibility and Adaptability	• Is the access control system capable of dynamically interposing access control rules based on system states? • Is the access control system capable of handling the evolution of the organisation's future access control policy changes?
Scalability	How scalable is the access control system? The metric for this criterion is either low, middle or high, depending on the number of roles or responsibilities that can be associated with the permission
Support for User mobility	Does the access control system allow users to access resources from different places within the healthcare organisation, from different institutions of even from home?
Reliability	How reliable is an access control system based on permission administration? In case of reliability, RBAC is considered to be more reliable as permissions are administratively associated with roles and users are made members of appropriate roles. On the contrary, any system that evaluates contexts before making an access decision is considered as less reliable since any compromise into context data will lead to wrong evaluation of context conditions and thus incorrect role assignment results in access permission that affect the security of the system
Emergency Access	Is access control system capable of bypassing access rules for critical access decisions?
Performance	Response time: • Does the response time of granting an access request meet the organisation's requirement? • Does the response time for the maximum number of access requests in an expected time frame meet the organisation's requirement? • Does the response time for activating and revoking access rules meet the organisation's requirements? Authentication function: • Can the access control system be integrated with or support identification authentication system? For response time, the metrics were assigned the following numbers: Low =1 , Moderate = 2 and High = 3

7.2 Evaluation of Access Control Mechanisms

This section examines the characteristics of access control mechanisms based on criteria discussed in Section 7.1, and summarised in Table 7.1. It can be inferred from the results presented in Table 7.2 that, Role-Based Access Control (RBAC) is a reliable model that greatly simplifies security management for system administrators and complex security policies can be applied more easily. On the flip side, RBAC uses static security mechanisms, the model is less flexible, provides no support for user mobility and does not contain a procedure for emergency access requests.

Table 7.2: Evaluation of Access Control Mechanisms

Mechanism	**Granularity of control**	**Dynamicity**	**Flexibility & Adaptability**	**Scalability**	**Support for user mobility**	**Reliability**	**Emergency Access**	**Performance (response time)**
RBAC	course-grained	Static	Low	Low	No	High	No	High
DRBAC	fine-grained	Dynamic	Moderate	Moderate	Yes	Moderate	No	Moderate
CBAC	fine-grained	Dynamic	High	High	Yes	Moderate	No	Moderate
PBAC	fine-grained	Dynamic	Moderate	Moderate	Yes	Low	No	Low
TBAC	fine-grained	Dynamic	High	High	No	High	No	Not known
TMAC	fine-grained	Dynamic	High	High	No	High	No	Not known
RoC-BAC	**fine-grained**	**Dynamic**	**High**	**Moderate**	**Yes**	**Moderate**	**Yes**	**Moderate**

KEY:

RBAC – Role-Based Access Control (Sandhu *et al.*, 1996)

DRBAC – Dynamic Role-Based Access Control (Zhang & Parashar, 2003)

CBAC– Context-Based Access Control (Covington *et al.*, 2001)

PBAC – Proximity-Based Access Control (Ardagna *et al.*, 2006)

TBAC – Task-Based Access Control (by (Thomas & Sandhu, 1998)

TMAC – TeaM-based Access Control (Thomas & Sandhu, 1993)

RoC-BAC – Role and Context Based Access Control (Omary, PhD Thesis 2014)

The Dynamic Role-Based Access Control (DRBAC) is an extension of the traditional RBAC model designed to addresses access control requirements for pervasive grid applications (Zhang & Parashar, 2003). These include: fine-grained access control, support for dynamic, seamless and secure interactions between participating entities. Furthermore, access privileges of an entity should depend on credentials, context or current state. With these requirements implemented, DRBAC model was therefore regarded as a fine-grained, and dynamic access control mechanism that supports user mobility. In comparison to a traditional RBAC model, DRBAC is also less flexible, does not scale well, less reliable, performs less as it incorporates an evaluation of contexts in access decisions, and it does not contain procedures to allow its users to bypass access rules in case of an emergency.

Covington *et al.* (2001) introduced Context-Based Access Control (CBAC) in Ubiquitous Computing to show how a well-developed notion of roles can be used to capture security-relevant context of the environment in which access requests are made. The authors introduced environment roles to create a uniform access framework that can be used to secure context-aware applications. Ardagna *et al.* (2006) proposed a mechanism called Proximity-Based Access Control (PBAC) for providing automated access to resources in a hospital emergency department environment. The PBAC model makes access decisions based on the proximity of the user to a particular resource such that when the user arrives in the proximity of the resource, access with the appropriate privileges is automatically granted. The user mobility in PBAC is highly supported using different proximity zones (Ardagna *et al.*, 2006).

Task-Based Access Control (TBAC) is a flexible access control mechanism, which has been widely implemented in workflow management systems (Thomas & Sandhu, 1998). In TBAC, permissions are assigned to tasks and users can only obtain the permissions during the execution of tasks. Unlike RBAC, TBAC supports type-based

and usage-based instances of tasks to control access to resources (Sandhu & Park, 2003), (Lu *et al.*, 2008). TeaM-based Access Control (TMAC) is an approach for applying role-based access control in collaborative environments where access permissions are specified on a "team" of collaborating users acting on various roles (Thomas & Sandhu, 1993). TMAC preserves the advantage of simpler security administration that RBAC-style models provide, and it also offers the flexibility to activate permissions for individual users and objects. The model, however, lacks the self-administration of assignment relations between entities.

Role and Context-Based Access Control (RoC-BAC) model was designed to address generic access control requirements for healthcare environments while at the same time supporting the continuity of care. In particular, RoC-BAC model was designed to allow health care workers to bypass access rules in an accountable manner in case of unexpected (or emergency) access requests. Among others, important access control requirements in a healthcare environment include support for emergency access procedure, auditing and alerting of accesses. Henceforth, the RoC-BAC model extends the traditional RBAC model with contexts and obligations, and a notion of health-related contexts is introduced. Permissions in RoC-BAC are assigned to roles, which are grouped into user roles and context roles. The subsections below present an evaluation of different access control mechanisms with respect to criteria discussed in Section 7.1.

1. **Granularity of control:** RBAC makes use of roles as the only context information in making access decision, hence it is considered a course-grained access control model. Dynamic Role-Based Access Control (DRBAC), on the other hand, uses multiple context information to monitor the context of different subjects or users. Context constraints are applied before assigning roles to the subject or user. In Context-Based Access Control (CBAC), access privileges are assigned dynam-

ically when the context (such as location, time, role, authentication trust level and types of information accessed) changes (DuraiPandian *et al.*, 2006). Similar to CBAC, the PBAC model is highly dependent on the context of the system to track dynamic changes. The context information in PBAC are grouped into three categories: user context (which may include location of the user (proximity) and user's capabilities), resource context (for example, capability of the resource and current load on the resource) as well as environmental context (such as, number of users in proximity of a resource at a given time) (Gupta *et al.*, 2006).

Furthermore, the TBAC model takes into consideration subject information, object information, time of use, usage count and executing tasks as appropriate context information before making access decisions. TMAC makes use of several context information, such as time, shift and location, while modeling access control policies. Like PBAC, contexts in Role and Context-Based Access Control (RoC-BAC) model is grouped into four: subject contexts, object contexts, environment contexts and health-related contexts. Based on the number of contexts supported in each access control model, only RBAC is considered to be course-grained while the remaining access control models are fine-grained.

2. **Dynamicity:** RBAC model is mostly static as users are assigned to specific roles and this assignment can only be modified by the system administrator. However, in the highly dynamic and heterogeneous environment, the access privileges of an entity depends not only on a role but also on its credential, context and current state. The Dynamic Role-Based Access Control (DRBAC) fulfils these requirements by adding dynamicity to the role assignment. The degree of dynamicity in this model is, however, not clearly defined as it depends on context sensing and processing capabilities in an application scenario (Zhang & Parashar, 2003). The CBAC is also considered as a dynamic model since different set of access rules are

applied when context changes. It provides dynamic binding of resources, that is, when a user moves from one domain to another, different sets of access rules will be executed before granting access to the resource.

PBAC, TBAC and TMAC are also dynamic models. In PBAC, specific permissions will be granted at run time when an individual user approaches a resource physically in a proximity zone, depending on the load and capability of the resource and the number of users in proximity of that resource at that particular time (Gupta *et al.*, 2006). The TBAC model allows for trustee sets and protection states to be modified dynamically (Chou & Wu, 2004). To illustrate its use, Aljareh & Rossiter (2002) showed how TBAC can be used in collaboration networks and argues that a person executing a task can be changed on the fly if required. Furthermore, TMAC provides fine-grained control over permission activation to individual users and objects. It is an active model of access control as permissions are activated at run-time, based on the context (Thomas, 1997). RoC-BAC is a dynamic model that allows health care workers to specify context (referred as reason throughout Chapter 6) and thus creating new access rule to allow an access to patient data and thus maintain the continuity of care.

3. **Flexibility and Adaptability:** RBAC model has low flexibility as it makes use of a single context information in its access decision. Compared to RBAC, the DRBAC model is more flexible as complex context-aware authorisation policies can be specified at design time. Context type definition and implementation are independent of the specification of access rules, and this makes DRBAC flexible and extensible. Like DRBAC, PBAC couples an access control solution with context information. It defines a set of access control policies that can easily be adopted to different contexts which makes the model flexible.

   In CBAC, the dynamic binding of resources when new scenarios arise makes the

scheme flexible. It provides a policy adaptation mechanism to ensure smooth flow of operations in new scenarios as well as rules to adopt to unforeseen events (Toninelli *et al.*, 2009). TBAC is flexible in the sense that, it allows a single activity or group of activities to share the same policy, and any member of a trustee set can be granted access. TMAC is a hybrid access control model that incorporates the advantages of a broad role-based permission assignment and administration across object types as in RBAC and yet it provides the flexibility for the fine-grained activation of permissions for individual users on individual object instances. The RoC-BAC model on the other hand has been integrated with contexts (in particular subject contexts, object contexts, environment contexts and health-related contexts) to allow users to specify health-related reasons behind their request to access patient's data that they are unauthorised in normal accesses. This capability makes RoC-BAC more flexible and adaptable than the traditional Role-Based Access Control (RBAC) model.

4. **Scalability:** RBAC is not highly scalable as access permission to information is limited to the number of responsibilities or roles assigned to a user. Besides, according to Karp *et al.* (2009) when the number of roles and permissions go beyond the order of thousands, there is a degradation of performance and the overall management of RBAC becomes difficult to handle. The concept of role hierarchy is included in DRBAC model such that new role can be created and extended from existing ones. The DRBAC system has a limitation, since it is role-scalable down the hierarchy. But with very large number of users, having dynamic roles, the DRBAC model will be resource greedy in terms of memory and processing. The PBAC model can be made scalable by using n-tier proximity zones around the resource instead of a single proximity zone (Gupta *et al.*, 2006). Different access privileges will then be given in different zones. Increasing the capabilities of the

resources also helps to accommodate more users in the proximity zones.

The CBAC model can be scalable assuming the infrastructure built is based on modular components which can be fully integrated in a broader pervasive architecture. Moreover, DuraiPandian *et al.* (2006) proposes an application of an Educational system for its architecture which can be easily extended. TeaM-based Access Control (TMAC) is a model proposed by Thomas (1997). Its advantage over other access control models such as RBAC is that, it is able to leverage the scalable security administration benefits of role-based permission assignment and yet able to provide fine-grained permission activation and deactivation to individual users and object instances. As an example, the system can assign and administer broad permissions for doctors on object types based on some role definitions and yet activate doctor's permissions to a patient's records (object instances) only when a doctor is taking care of the patient.

The work by Thomas & Sandhu (1993) discusses the usage of authorization subtasks where a subtask is assigned to a single transient object. This makes TBAC scalable in two ways. The first is that TBAC can handle increased workload. As the workload increases, an authorisation step can spawn authorisation subtasks taking care of various requests for authorisation. The second way is that, TBAC can handle increasing complexity of the authorisation steps. In Thomas & Sandhu (1998) a family of TBAC models is presented with a basic model used to build composite ones with additional constraints.

5. **User mobility:** Since the only context information for the RBAC model stems from the user, a change in user location will not cause any change in role assignment. RBAC has, therefore, no support for user mobility. The DRBAC model supports user mobility since the user's role can change with different context conditions. The PBAC scheme supports user mobility only when an individual user moves in

a specific zone. Access privileges are removed as soon as the user moves out of the zone (Gupta *et al.*, 2006). In certain circumstances, this behaviour of PBAC can be beneficial especially when people are in a hurry and move out from an ongoing session or even forget to logout (Bardram, 2004).

In CBAC, resources are integrated with context information under which they should operate. Support for user mobility is applicable in boundaries where context rules have been attached to resources. TBAC and TMAC, which are a special configuration of RBAC model, have no support for user mobility since access controls are restricted to tasks and teams respectively. The RoC-BAC model, on the other hand, allows specification of location-based and temporal-based access rules and thus supports moderate user mobility by evaluating dynamic context information while making access decision.

6. **Reliability:** In RBAC, access permissions are administratively associated with roles and users are made members of appropriate roles. Thus, the management of authorisation in RBAC is quite simple and static, making RBAC reliable. In DRBAC, the reliability of context information security is a key issue. Corrupted contextual data will lead to wrong evaluation of context conditions, thus incorrect role assignment results in access permissions that affect the security of the system. While the reliability of the PBAC scheme is tied to the accuracy of the positioning system used, this accuracy depends on electromagnetic environment and varies over time. PBAC can make use of error contour maps around the proximity zone to compensate for errors of the positioning system (Gupta *et al.*, 2006).

   For other models like CBAC, reliability is still an issue. When there is a new scenario where the policy adaptation mechanism will be triggered, there is no guarantee that the new access rules applied are most optimal or correct. TBAC dynamically manages permissions as authorisations progress to completion. Au-

thorisations in TBAC have strict usage, validity and expiration characteristics that may be tracked at runtime, thus making the model more reliable. TMAC, on the other hand, can be used to restrict access to information and functionality in the shared environment to those trusted. It can be used to help coordination by providing only those functions to team members that are currently needed to fulfil their roles. However, managing access permissions assigned to members of dynamic and emerging teams with frequently changing processes raise significant issues. The reliability of TMAC, therefore, depends on how dynamic the teams and processes are. Similar to other context-based models, RoC-BAC model is less reliable than the traditional RBAC model since access permission depends on context and corruption of context data or even wrong specification of health-related contexts (or reasons) will result into wrong authorisation.

7. **Emergency Access:** The healthcare domain follows the "care comes first principle" where patient's health care needs are to be put first before anything else. With this principle in place, an access control system in the healthcare organisation should be designed in such a way that infrequent access requests involving emergency situations are handled by overriding existing access rules. If there is a patient who was injured as a result of a road accident, for instance, the nearest qualified healthcare professional should be able to access the patient's basic medical data and provide appropriate care as seen appropriate. This should be possible even if a healthcare professional is not directly associated with the patient. Out of seven access control models discussed herein, this significant access control requirement for the healthcare domain is only enforced by the Role and Context-Based Access Control (RoC-BAC). The proposed RoC-BAC model extends the traditional Role-Based Access Control model with contexts and obligations to allow healthcare workers to bypass access rules in case of unexpected (emergency) access requests

so as to ensure the continuity of care.

8. **Performance:** The fact that RBAC uses only one context information, allows the scheme perform better than its counterparts. DRBAC, for instance, depends on several factors, such as number of roles assigned, number of permissions allocated to each role, rate at which transitions occur between roles and frequency of context changes. The performance overhead of DRBAC has been experimentally evaluated in Zhang & Parashar (2003), and its implementation in an application shows higher operational complexity. Similarly, the performance of PBAC scheme varies with the system context, including: capability of the resource, the load of the resource and the number of users in the proximity zone. Gupta *et al.* (2006) define a parameter termed "window-of-opportunity" that defines the maximum delay that can be allowed to take corrective action. This delay can be used to evaluate the performance of PBAC with varying context information.

   In CBAC model, fast response time is one of its basic requirements. With different filtering levels and a set of rules which need to be executed, performance issues can arise and different means have to be devised to optimise search. Pigeot *et al.* (2007) introduce one way to increase performance through the implementation of a history module which acts as a cache. Currently, only limited performance and complexity evaluations have been carried out on access control models like TBAC and TMAC. Section 7.3 presents the results of performance evaluation, by analysing overheads introduced by different entities and relations in a CEATH system (implementing Role and Context-Based Access Control (RoC-BAC)) against those of EMR-RBAC system (implementing Role-Based Access Control (RBAC)).

7.3 Performance Evaluation

This section presents the results of performance evaluation, performed on both CEATH and EMR-RBAC systems. These experiments were carried out to identify the effect of new elements and relations introduced on RoC-BAC from a traditional RBAC model. This Section is divided into two: Section 7.3.1 discusses experimental set up and Section 7.3.2 analyses the results from the experiments.

7.3.1 Experimental Set up

For the experiments, the number of patients medical records used in both systems were 95,141. There were also a total of 50 scenarios collected from the Tanzania healthcare system to test the effect of new elements and relations introduced in RoC-BAC model against that of the traditional RBAC approach. The scenarios were also used to evaluate the accuracy of the system.

To begin with, the following were considered as the cause of delay during execution in RoC-BAC:

- Number of roles assigned to a subject or object
- Number of permissions assigned to a role
- Number of context(s) to be evaluated

Each of these factors have been discussed in detail in Section 7.3.2.

7.3.2 Experimental Results and Analysis

This section presents the results of the performance analysis conducted on two prototypes, EMR-RBAC and CEATH, which implements RBAC and RoC-BAC respec-

tively.

1. **Number of Roles:**

   In this experiment, response time in relation to a number of roles assigned to a subject or object are measured. This experiment was conducted in order to identify if there is any effect introduced by the access control model's mapping. In this experiment, each user of the system was assigned five roles and these roles were associated with permissions. The role with highest privileges had five permissions. The analysis from this experiment indicates that, response time increases as the number of roles assigned to a user increases. Between the two access control models, it takes three times as much time to execute an access request in RoC-BAC compared to an execution in RBAC. The indicative performance results on the number of roles assigned to a subject for the four selected users in both RBAC and RoC-BAC are summarised in Table 7.3 and 7.4, and also presented in Figure 7.1 and 7.2.

No. of roles	**Response Time (ms.)**	
	RBAC	**RoC-BAC**
1	0.02640	0.08596
2	0.02440	0.06597
3	0.02625	0.07125
4	0.02107	0.06656
5	0.02560	0.06406

No. of roles	**Response Time (ms.)**	
	RBAC	**RoC-BAC**
1	0.02294	0.07317
2	0.02336	0.06442
3	0.02467	0.08356
4	0.02093	0.07160
5	0.02444	0.08418

Table 7.3: Response times for the first user (left) and second user(right)

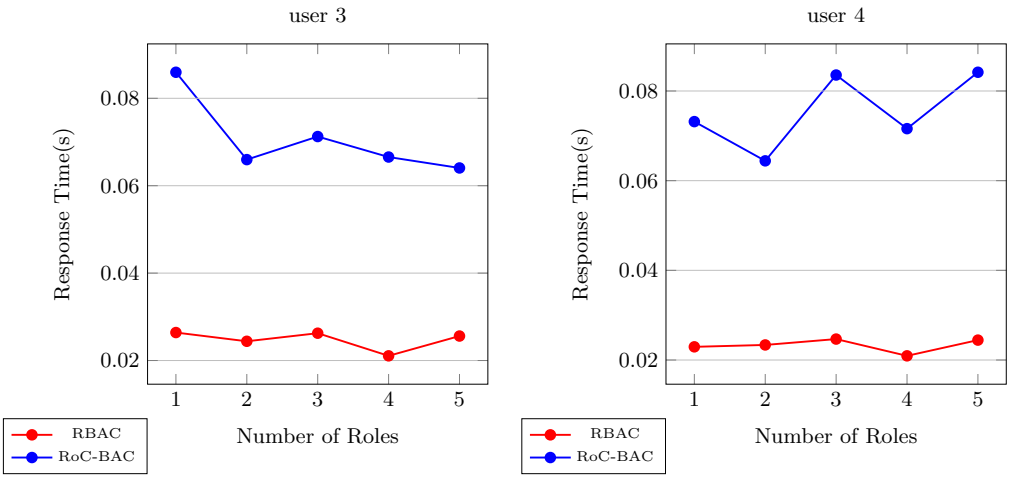


Figure 7.1: The performance results on the number of roles assigned to a subject for the first two users

No. of roles	Response Time (ms.)	
	RBAC	RoC-BAC
1	0.02694	0.06422
2	0.02385	0.06789
3	0.02570	0.06899
4	0.02760	0.07571
5	0.02623	0.06519

No. of roles	Response Time (ms.)	
	RBAC	RoC-BAC
1	0.02040	0.06419
2	0.02170	0.06833
3	0.02200	0.07606
4	0.02347	0.07016
5	0.02360	0.07139

Table 7.4: Response times for the third user (left) and fourth user(right)

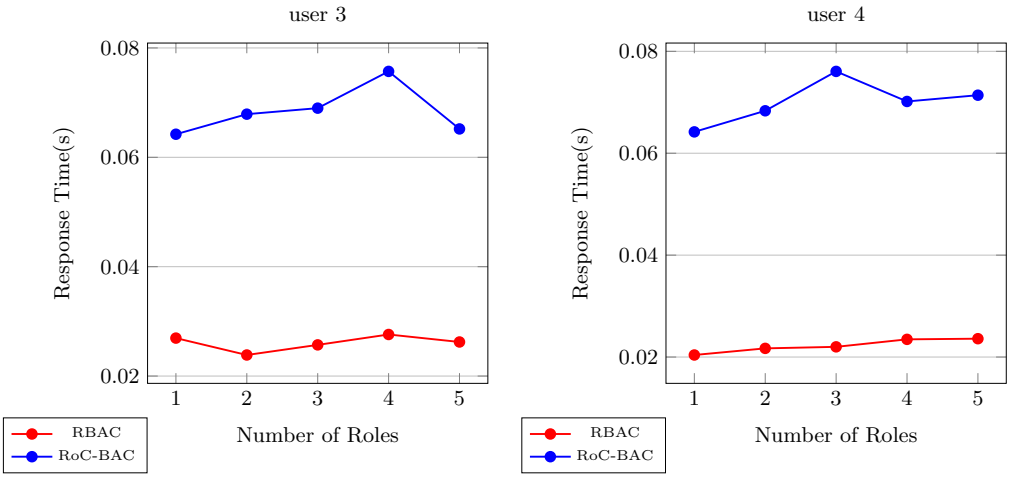


Figure 7.2: The performance results on the number of roles assigned to a subject for the third user (left) and the fourth user (right)

2. **Number of Permissions:** In this second set of experiments, each user had a state machine with five roles, and a role with highest privileges was set to be an active role. The number of permissions assigned to an active role were varied. The response times for different number of permissions are in Table and Figure 7.3.

No. of Permissions	Response Time (s.)	
	RBAC	RoC-BAC
0	2300	8440
5	2500	8400
6	2602	7766
7	2698	8405
8	2804	8631
9	2912	8733

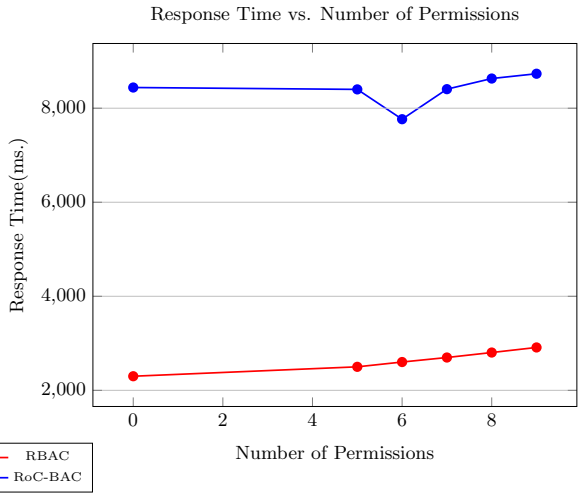


Figure 7.3: Number of permissions assigned to a role

3. **Performance against Location and Time:** In this third set of experiments, the performance of CEATH was evaluated when an access rule contains both location and timing constraints. An example of such access rule is: "Doctor John Doe requests to access Bob's medical records from his office at 11:40 a.m". To find the mean response time, five scenarios with varying location and timing information were defined, and each scenario was executed ten times. The average response time for each access request sent was measured at 0.0368614 ms. Figure 7.4 depicts response time in CEATH system when an access policy contains location and timing information.

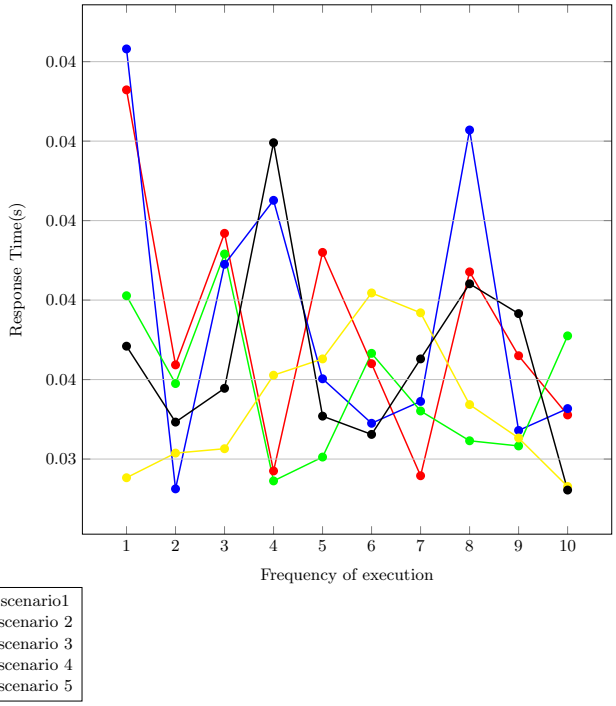


Figure 7.4: The effect of location and timing on performance of the CEATH system

The following is a list of five scenarios used in this experiment

(a) scenario 1: a nurse from physiotherapy department is requesting to access patient A's medical records from the front desk

(b) scenario 2: a user with role doctor is requesting to access patient C's medical records from his office within the hospital at 1:00 p.m.

(c) scenario 3: a user with a role physiotherapy doctor is requesting to access patient C's medical medical records from his home office (outside the hospital) on Saturday afternoon at 12:30 p.m.

(d) scenario 4: a senior nurse who is in the same ward as the patient is requesting to access patient X's medical records during the morning working shift

(e) scenario 5: a consultant surgeon is requesting to access patient E's medical

Table 7.5: Response time for access policies with health-related contexts

Frequency	SCENARIO [time in ms.]				
	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
1	0.03877	0.0382	0.03698	0.03339	0.02849
2	0.32687	0.03734	0.03778	0.03258	0.0285
3	0.03255	0.03947	0.03783	0.03059	0.02808
4	0.03791	0.03589	0.03897	0.02701	0.03484
5	0.03083	0.03713	0.03808	0.0274	0.03164
6	0.03108	0.03656	0.03727	0.02676	0.02664
7	0.03133	0.03164	0.03743	0.03172	0.02698
8	0.0396	0.03886	0.0386	0.02804	0.02845
9	0.02798	0.03593	0.03796	0.02685	0.02717
10	0.02658	0.03801	0.02654	0.02699	0.02926

records from a clinic which is outside the hospital environment.

4. **Performance with Health-Related Contexts:** To make sure that healthcare professionals' are able to access medical records during unexpected (emergency) situations, this thesis introduces a new concept called health-related contexts into its access control decisions. The health-related contexts are integrated into Role-Based Access Control model so as to make RoC-BAC model flexible and fine-grained for the healthcare domain. To measure performance overhead introduced by health-related contexts, this section presents the results from Role and Context-Based Access Control (RoC-BAC) mechanism, which was implemented in CEATH system.

   Moreover, different context-based access rules were used during this experiment. The average response time for five scenarios, with each being executed ten times is 0.038827 ms. Table 7.5 presents the response times for five scenarios executed ten times. It is also worth noting that, the response time when an access request contains location, time and health-related context is higher compared to an av-

erage time when an access request contains only location and timing information (shown in Figure 7.4). This is due to the fact that the usage of more contexts in an access request involves longer access evaluation. This thesis, therefore, shows that, the more contexts specified in an access request, the longer it takes for an access control system to execute. Although the proposed role and context-based system is slower compared to pure role-based system, functional trade-off between performance and proper access for the domain were considered, and thus RoC-BAC is regarded as a more appropriate mechanism for the healthcare environment. Figure 7.5 summarises the impact of location, time and health-related contexts on the performance of RoC-BAC.

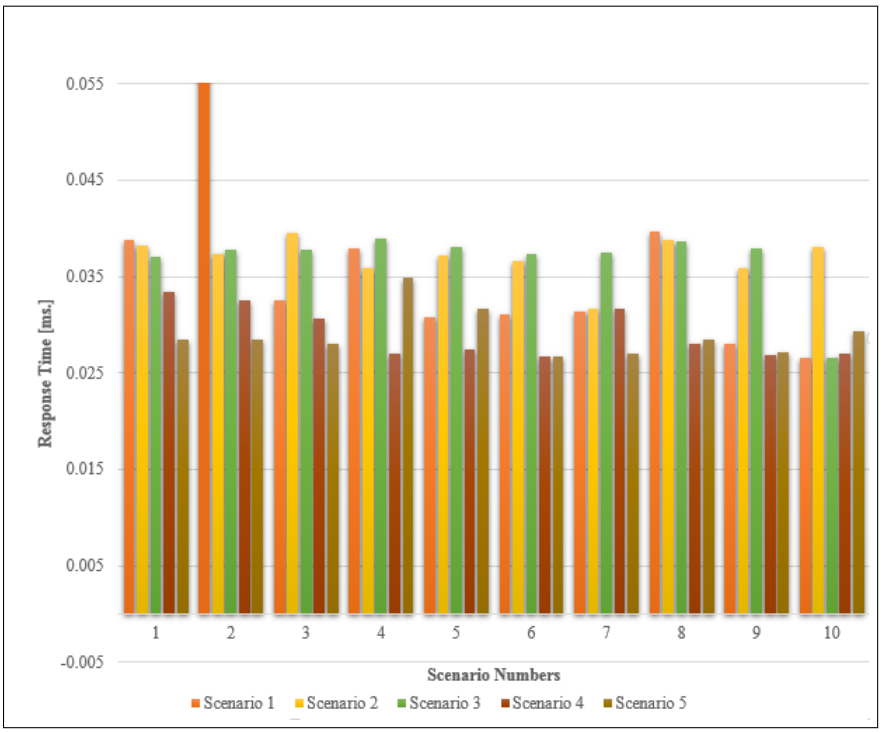


Figure 7.5: Impact of location, time and health-related context in performance

The following is a list of scenarios used to measure the performance of the CEATH system when health-related contexts are specified in an access request. More scenarios collected for evaluation of the systems are listed in Appendix C.

(a) A consultant requests to access patient A's medical records after being admitted to the hospital following an accident in the mines

(b) A nurse requests to access medical records of a woman who has been attacked by her live-in partner in a gender-based violence instance.

(c) In rural Tanzania, a midwife is requesting to access medical records of a fifteen years old girl who is having complications in during labor and delivery

(d) A clinical assistant is requesting to access medical records of a girl who is in critical condition following non-surgical cutting of her female genitalia

(e) A senior nurse is requesting to access medical records of a high school student who is in critical condition following attempted abortion by unskilled abortionist.

Furthermore, in relation to specification and evaluation of access rules between the two systems (that is, CEATH which implements RoC-BAC and EMR-RBAC which implements traditional RBAC approach), CEATH would be able to accommodate more rules than the traditional role-based system. In case of fifty (50) access requests listed in Appendix C with 28 of them containing dynamic context information (in Appendix C.2) and the remaining 22 with no context information (in Appendix C.1), CEATH system would be able to accommodate all fifty cases as the model itself is an extension of the traditional RBAC model and hence allows the usage of role-based access rules. The EMR-RBAC would, however, accommodate only 22 requests.

7.4 Expert User Evaluation

The aim of this third and final phase of the evaluation was to evaluate the usability of the Role and Context-Based Access Control (RoC-BAC) system prototype named

CEATH (Context-Enhanced Access in a Tanzania Healthcare) and to carry out heuristic or guideline-based evaluation of the system. The main objective was to identify general problems with the newly proposed Role and Context-Based Access Control (RoC-BAC) model and also to identify specific usability problems associated with the CEATH system.

7.4.1 Apparatus

All tests were carried out in a closed environment, a room within a hospital. The room was fitted with one machine running our prototype and another running a system that implements a Role-Based Access Control (RBAC) model.

7.4.2 Participants

Eight users were recruited from three large hospitals in the United Republic of Tanzania. Five of the experts were from the Muhimbili National Hospital (MNH), two from the Kilimanjaro Christian Medical Centre(KCMC) and one from the Bugando Medical Centre. For the analysis, users were divided into two groups: two were amateurs with up to three years of experience and the remaining six contained of semi and full professionals with up to thirty years of knowledge in the healthcare domain. The latter group included expert users who gave expert opinions on aspects of the system.

7.4.3 Test Description

A prototype was designed and implemented and test scenarios were designed, based on typical tasks the system was intended to perform, that is normal accesses and infrequent accesses involving emergency situation. Users were asked to comment, ask questions, or ask for help freely at any stage of the evaluation.

7.4.4 Scenarios and Questions

The CEATH's evaluation consisted of two scenarios followed by questions specific to the CEATH system. The first scenario required the user to step through a normal access request task using the browser-based interface of the system. The task involved requesting access to medical records of the patient that a healthcare professional has defined relationship using normal access procedure, implemented using the Role-Based Access Control (RBAC). The second scenario involved specifying health-related contexts to access medical records of a patient that a healthcare professional has no prior relationship with. Timings for each scenario was collected, and the user was asked to rate the usability of each system and specific questions related to the representation of information and data in CEATH system.

7.4.5 Results and Discussion

The evaluation showed that the usability of the CEATH system as a whole is good. As shown in Figure 7.6, a System Usability Scale with ten item questionnaire with 5 response options (1 for strongly disagree and 5 for strongly agree) was used to evaluate the usability of the CEATH system (Brooke, 1996). Out of ten questionnaire items listed below, nine items are normally used to evaluate general usability and one (number ten item) is used to evaluate learning. Figure 7.7 shows a graphical representation comparing the overall usability of CEATH, which implements RoC-BAC, and EMR-RBAC which implements the RBAC model. The ratings given by each user for each question were added, giving the overall impression of the distribution of ratings for each system.

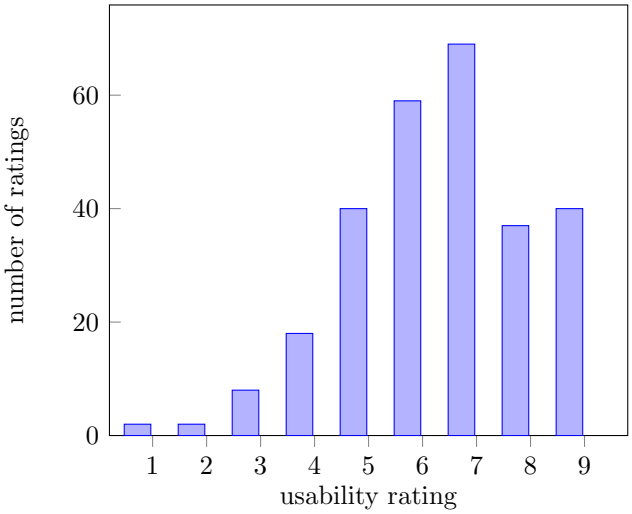


Figure 7.6: Usability of the CEATH system using System Usability Scale

1. I think that I would like to use this system frequently
2. I found the system unnecessarily complex
3. I thought the system was easy to use
4. I think I would need the support of a technical person to be able to use this system
5. I found the various functions in the system were well integrated
6. I thought there was too much inconsistency in this system
7. I would imagine that most people would learn to use this system very quickly
8. I found this system very cumbersome to use
9. I felt very confident using the system
10. I needed to learn a lot of things before I could get going with this system

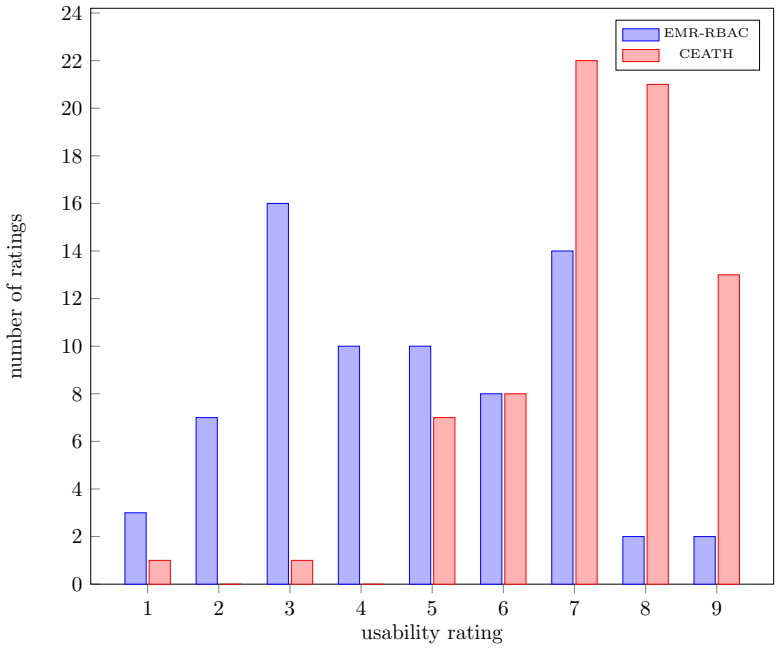


Figure 7.7: Usability Evaluation of the EMR-RBAC and CEATH systems

The CEATH system was favoured by the users over the traditional approach implemented in EMR-RBAC system. Users rated the system as easier to user, easier to understand and also appropriate for the domain. On the negative side, users felt the system would involve some performance issues as a result RoC-BAC's support for n contexts that can be evaluated by the system. This concern is, however, not considered as a significant issue since the majority of the users trusted the system to achieve its goal of using different access mechanisms for different access requests.

Valuable user feedback was gathered through comments and suggestions and these will inform design decisions for future versions of the CEATH system, and may include addressing issues in relation to user interaction, evaluation of contexts using the machine learning to make the system context-aware and also visualisation of the underlying processes. In summary, the evaluation showed that CEATH represents an important step towards a system in the healthcare domain that could help healthcare

professionals to access medical records of the patients in an accountable manner, and thus ensure the continuity of care in the domain where shortage of human resources for health is common.

7.5 Analysis and Discussion

The criteria for evaluating access control systems proposed by Hu & Scarfone (2012) from the National Institute of Standards and Technology (NIST) were used to analyse the capabilities of access control mechanisms. The criteria used in this thesis include granularity of control, dynamicity, flexibility and adaptability, scalability, support for user mobility, reliability, support for emergency access procedure, as well as performance. Based on these criteria, the proposed RoC-BAC model is regarded as a fine-grained, flexible and dynamic access control model that moderately supports user mobility and also allows health care professionals to bypass access rules in case of an unexpected (infrequent) situation.

The second part of the evaluation involved comparative analysis in relation to the performance of two access control models, RBAC and RoC-BAC. The results in this part indicate that the integration of contexts into RoC-BAC introduces some performance overheads due to the fact that access decisions in a system implementing the proposed RoC-BAC approach involves more evaluation factors in terms of contexts than that of a traditional RBAC model. Even though RoC-BAC seems to introduce trivial performance overhead, the overall approach was designed based on access control requirements gathered from the healthcare domain and thus its approach is more appropriate than the traditional RBAC.

Another significant finding from performance evaluation of the RoC-BAC approach is that, delays during access to medical records were due to various factors including:

number of roles assigned to subjects and objects, number of permissions in an active role as well as frequency of events. Additionally, it was noted that the more contexts integrated into the RBAC forming RoC-BAC, the more performance overhead the system experiences, and the better the system becomes in terms of access control for the healthcare domain. The validity of this statement can be verified by performance evaluation results of the RoC-BAC model while evaluating access rules containing location and time information (with an average of 0.0368614 ms) which is slightly lower than response time for an access request that contains location, time and health-related contexts (an average of 0.038827 ms). The expert user evaluation was the third and final part of the evaluation. The results obtained indicate that CEATH which implements RoC-BAC model is favoured due to its ability to provide access in two different levels (both normal and for infrequent access requests) than the traditional RBAC approach.

7.6 Conclusions

In this chapter, experimental results for evaluating the proposed Role and Context-Based Access Control (RoC-BAC) model are presented and discussed. Two prototypes, namely EMR-RBAC and CEATH (that is, Context-Enhanced Access in a Tanzania Healthcare) which have been designed and implemented in Chapter 6, were used for evaluation. The chapter began with a review of criteria proposed by the National Institute of Standards and Technology (NIST) that can be used to evaluate access control systems. The evaluation criteria used in this thesis include granularity of control, dynamicity, flexibility and adaptability, scalability, support for user mobility, reliability, emergency access and performance.

As the proposed Role and Context-Based Access Control (RoC-BAC) extends the traditional Role-Based Access Control (RBAC) model with multiple contexts into its

access decision and obligations, the model is therefore characterised as fine-grained, flexible and adaptable. The model also moderately supports user mobility and contains a procedure for infrequent (emergency) access requests. On the contrary to a pure role-based system, a role and context-based system supports the continuity of care by allowing healthcare professionals to bypass access rules in an accountable manner by specifying health-related contexts in case of an infrequent access request associated with an emergency situation. From an analysis of the performance of the two systems, this thesis has shown that RoC-BAC introduces trivial performance overhead than a pure role-based system since its access decision involves an evaluation of multiple contexts. Chapter 8 concludes this thesis.

Chapter 8

Conclusions & Future Work

This chapter concludes the thesis. A summary of research is presented in Section 8.1, and suggestions for future research directions are in Section 8.2.

8.1 Research Summary

Access control is an important aspect of any information system. It is a way of ensuring that authenticated users can access only what they are authorised to and no more. In other words, it grants authenticated users access to resources based on organisation policies and permission levels assigned to each user or user group. As a research area, access control has been extensively studied in academia and in industry, and thus a wide range of access control models, mechanisms and systems have been proposed. However, despite its success, specific access control requirements for the dynamic and collaborative environments like healthcare that needs to support the continuity of care to patients have not been addressed. This results in a wide gap between what is required and what is actually practised in the domain. As a result of this gap, access control policies implemented in the healthcare domain are considered to be too restrictive and affect the continuity of care to patients in case of a shortage in healthcare professionals.

To address diverse access control requirements, current solutions to this problem have been built on traditional access control models such as Role-Based Access Control (RBAC). These models contain numerous limitations for their use in electronic healthcare information systems to support the continuity of care. As an example of a traditional access control mechanism, Role-Based Access Control (RBAC) model is a powerful tool for specifying and enforcing organisational policy in a way that seamlessly maps to an enterprise structure. It is a policy neutral authorisation approach suited for large-scale enterprises. On the negative side, RBAC is static, since it makes access control decisions based on users' attributes such as identities and it does not take into account contexts while determining whether access to a resource should be allowed or not.

From the proposed Contexts, Organisational rules, e-health Initiatives and Legislative rules (COIL) methodology for gathering access control requirements for the healthcare domain, this thesis argues that an access control system designed for the healthcare domain should contain contexts, privacy and security capabilities, and organisational and legislative rules. The designed access control model for domain should also be fine-grained and flexible enough to allow healthcare professionals to bypass access rules in an accountable manner in case of unexpected emergencies.

8.1.1 Summary of the Main Conclusions

This thesis has focused on the development of a new context-based access control model that addresses access control requirements for the healthcare domain. This section summarises the main conclusions. The introductory Chapters 1 and 2 are excluded from the discussion, because they do not contain any new research materials.

Chapter 3 dealt with an analysis of existing access control models and mechanisms for the modern electronic healthcare environment. The suitability of traditional access control models for the healthcare environment was analysed, and in this analysis Discretionary Access Control, Mandatory Access Control, Role-Based Access Control and Attribute-Based Access Control were evaluated. From the existing literature it was noted that discretionary access control, for instance, is not suitable for the modern electronic healthcare environment since the model is static , it lacks proper control of information flow and the owner of a particular object can pass access rights on that object to any other subject without any restrictions. Based on the limitations of existing access control models, the Chapter concluded with a proposal to design a context-based access control model for the healthcare domain, and the model should address appropriate access control requirements.

Prior to designing of a new access control model, this research focused on gathering

access control requirements for the domain. Chapter 4, therefore, discusses the development of a new approach named COIL for gathering comprehensive access control requirements for the healthcare domain. The COIL approach is a combination of four different areas of research that affect access to electronic medical records. The areas researched, which also form the COIL approach are contexts for a fine-grained access control model, privacy and security capabilities from national electronic health initiatives, organisational rules as well as legislative rules from selected legislations. Several privacy and security capabilities were proposed, and also included as part of the COIL approach. These include: user identification and authentication, authorisation, implementation of function for emergency access procedures, auditing and alerts, and patient consent. To test its validity and to show how the developed COIL approach could be used, the chapter also contains results of its evaluation.

Chapter 5 discusses the development of a new context-based access control model for the healthcare domain. The proposed model is named Role and Context-Based Access Control (RoC-BAC), and it is an extension of the traditional Role-Based Access Control model with health-related contexts and obligations. In addition to the new category of contexts, the proposed model also supports the specification of subjects contexts, objects contexts and environments contexts. This chapter also introduces a new concept of health-related contexts, that define healthcare domain's specific contexts that could be evaluated in an access control decision of a modern healthcare information system. Its evaluation in an access decision is expected to support the continuity of care by allowing healthcare professionals to bypass access rules in an accountable manner.

Chapter 6 discusses the development of two prototypes namely: CEATH, that implements Role and Context-Based Access Control (RoC-BAC) model, and EMR-RBAC that implements Role-Based Access Control. These prototype were designed and im-

plemented in order to achieve two main objectives. First and foremost, to demonstrate that the proposed Role and Context-Based Access Control model is practical and also to evaluate performance overheads introduced by new entities and relations. The later objective is achieved by comparing the performance of CEATH with the performance of EMR-RBAC. The system was also implemented to allow for expert user evaluations of the system

Chapter 7 discusses the results of an evaluation of CEATH system against that of EMR-RBAC. The chapter began by reviewing a list of criteria proposed by the National Institute of Standards and Technology (NIST) that could be used to evaluate access control systems. The criteria used include granularity of control, dynamicity, flexibility and adaptability, scalability, support for user mobility, reliability, emergency access functions and performance. From the first seven criteria, the proposed RoC-BAC model was concluded to be fine-grained, flexible, dynamic, provides support for user mobility, and implements emergency access function. For the comparative analysis on performance of CEATH against that of EMR-RBAC, it was noted that CEATH takes as much as three times to execute an access request compared to the time spent by the EMR-RBAC. However, despite the overheads, the system's ability to allow healthcare professionals to access to records in an unexpected emergency situations and thus ensure the continuity of care far outweighs any performance concerns. That being said, RoC-BAC model is considered to be appropriate solution for the domain that the conventional RBAC model. Chapter 8 summarises the thesis and points out areas for future research directions.

8.1.2 Contributions

The following are the contributions of this thesis to the body of knowledge:

1. A new approach for gathering comprehensive set of access control requirements

in a healthcare domain has been developed. In this research work, access control requirements for the healthcare domain were categorised into four main groups that have an impact on access to medical records. The access control requirements arose from legislations, privacy and security capabilities from national electronic health initiatives as well as rules that govern operations within the healthcare organisation and rules from the legislation. The COIL approach describes a step-by-step approach for specifying a comprehensive set of access control requirements for the domain.

2. A taxonomy of access control models was has been designed, and various access control models and mechanisms were classified against the proposed Role and Context-Based Access Control model.

3. To support the continuity of care by allowing healthcare professionals to bypass access rules in an accountable manner, this thesis proposes a context-based access control model called Role and Context-Based Access Control (RoC-BAC). The RoC-BAC model builds upon a traditional Role-Based Access Control by extending it with health-related contexts and obligations. In addition to the introduction of health-related contexts, RoC-BAC also supports subject contexts, object contexts and environment contexts.

4. With the proposed RoC-BAC model, a new concept of health-related contexts is also introduced. It represents specific contexts from the healthcare domain that should be evaluated by an access control system in order to support the continuity of care.

5. To demonstrate that the proposed RoC-BAC model is doable and also to evaluate the performance performance of CEATH, two prototypes (one implementing Role and Context-Based Access Control model and the other implementing Role-Based Access Control model) were implemented. From the performance analysis of the

two systems, this thesis argues that, even though RoC-BAC takes longer to execute access requests compared to that of RBAC model, provision of care is way more important in healthcare performance, and thus RoC-BAC is regarded as an appropriate approach for the domain which needs to ensure the continuity of care.

8.2 Future Work

In this thesis, an evaluation strategy for the proposed context-based access control model involved the usage of scenarios from Tanzania healthcare environment. This section discusses more work that can be carried out in the future.

1. **Automation of scenario generation:** To test the scalability of the scenarios generated for the domain, a system that contains four parts of the COIL approach can be developed as a future work. Such a system should contain contexts (subdivided further into its four main groups as proposed in this thesis: subject contexts, object contexts, environment contexts and health-related contexts). The three other parts of the system are: privacy and security capabilities from national electronic health initiatives, legislative rules as well as organisational rules.

2. **Automatic Evaluation:** The integration of a rule engine into the access control solution is another aspect of future work. Since the current prototype (that is, CEATH system) allows healthcare professionals to manually specify health-related contexts so as to bypass access rules, an automatic evaluation of context conditions can be carried out through an integration of a rule engine in to the overall access decision. The proposed engine should be able to evaluate access rules automatically and provide access without users' intervention. Additionally, machine learning approaches can be investigated and its solution be integrated into the system so as to learn and evaluate any new access scenario against a database of existing ones.

3. **Appropriate Help to Healthcare Professionals:** Since the proposed Role and Context-Based Access Control model allows healthcare professionals to bypass access rules in an accountable manner in case of an unexpected emergency situation, the system should also be able to offer healthcare professionals who have bypassed access rules appropriate help to complete their job. For certain circumstances in a Tanzania healthcare system where there is high shortage of healthcare professionals, it is common to find less skilled professionals seeking a change in access rights so as they could act as skilled professionals and hence provide basic services to the patients. As a future work, different types of help (such as a phone call from another healthcare professional or a guidance manual) to healthcare professionals should be identified against different categories of healthcare professionals, and those helps should be integrated into the system.

Abadi, M. & Fournet, C. (2003). Access Control Based on Execution History. In *NDSS*, vol. 3, 107–121.

Abel-Smith, B. & Rawal, P. (1992). Can the Poor Afford Free Health Services? A Case Study of Tanzania. *Health Policy and Planning*, **7**, 329–341.

Abowd, G., Dey, A., Brown, P., Davies, N., Smith, M. & Steggles, P. (1999). Towards a Better Understanding of Context and Context-Awareness. In *Handheld and Ubiquitous Computing*, 304–307, Springer.

Accenture (2012). Singapores Journey to Build a National Electronic Health Record System. Tech. rep., Accenture.

Alhaqbani, B. & Fidge, C. (2007). Access Control Requirements for Processing Electronic Health Records. In *Proceedings of the 2007 international conference on Business process management*, 371–382, Springer-Verlag.

Aljareh, S. & Rossiter, N. (2002). A Task-Based Security Model to Facilitate Collaboration in Trusted Multi-Agency Networks. In *Proceedings of the 2002 ACM Symposium on Applied Computing*, 744–749, ACM.

Allen, R. & Shatz, M. (1983). What says Meow?. The Role of Context and Linguistic Experience in Very Young Children's Responses to What-Questions. *Journal of Child Language*, **10**, 321–335.

Almenárez, F., Marín, A., Campo, C. & García R, C. (2005). TrustAC: Trust-based Access Control for Pervasive Devices. In *Security in Pervasive Computing*, 225–238, Springer.

Anderson, J.G. (2007). Social, Ethical and Legal Barriers to E-health. *International Journal of Medical Informatics*, **76, (5)**, 480–483.

Anderson, J.P. (1972). Computer Security Technology Planning Study. Volume 2. Tech. rep., DTIC Document.

Anderson, R.J. (1996). A Security Policy Model for Clinical Information Systems. In *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on*, 30–43, IEEE.

Ardagna, C.A., Cremonini, M., Damiani, E., di Vimercati, S.D.C. & Samarati, P. (2006). Supporting Location-Based Conditions in Access Control Policies. In *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*, 212–222, ACM.

Axiomatics (2013). Fine-Grained Authorization. `https://www.axiomatics.com/fine-grained-authorization.html`, [Online: accessed in 25- January- 2013].

Bacon, J., Moody, K. & Yao, W. (2002). A model of oasis role-based access control and its support for active security. *ACM Transactions on Information and System Security (TISSEC)*, **5**, 492–540.

Baker, D., Barnhart, R. & Buss, T. (1997). PCASSO: Applying and Extending State-of-the-Art Security in the Healthcare Domain. In *Proceedings of the13th Annual Computer Security Applications Conference*, 251–260, IEEE.

Ball, M.J. & Lillis, J. (2001). E-health: Transforming the Physician/Patient Relationship. *International Journal of Medical Informatics*, **61 (1)**, 1–10.

Bardram, J.E. (2004). Applications of Context-Aware Computing in Hospital Work: Examples and Design Principles. In *Proceedings of the 2004 ACM Symposium on Applied Computing*, 1574–1579, ACM.

Bardram, J.E. & Nørskov, N. (2008). A Context-Aware Patient Safety System for the Operating Room. In *Proceedings of the 10th International Conference on Ubiquitous Computing*, 272–281, ACM.

Baskerville, R. (1993). Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Computing Surveys (CSUR)*, **25 (4)**, 375–414.

Bazire, M. & Brézillon, P. (2005). Understanding Context Before Using it. In *Modeling and Using Context*, 29–40, Springer.

Becker, M. (2007). Information Governance in NHS's NPfIT: A Case for Policy Specification. *International Journal of Medical Informatics*, **76 (5)**, 432–437.

Bell, D.E. & LaPadula, L.J. (1973). Secure Computer Systems: Mathematical Foundations. Tech. rep., National Technical Information Service.

Bennett, C.J. & Raab, C.D. (2003). *The Governance of Privacy: Policy Instruments in Global Perspective*. Ashgate Publishing, Ltd.

Bertino, E., Bettini, C., Ferrari, E. & Samarati, P. (1996). A Temporal Access Control Mechanism for Database Systems. *IEEE Transactions on Knowledge and Data Engineering*, **8 (1)**, 67–80.

Bertino, E., Bonatti, P. & Ferrari, E. (2001). TRBAC: A Temporal Role-Based Access Control Model. *ACM Transactions on Information and System Security (TISSEC)*, **4 (3)**, 191–233.

Bertino, E., Catania, B., Damiani, M. & Perlasca, P. (2005). GEO-RBAC: a Spatially Aware RBAC. In *Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies*, 29–37, ACM.

Beznosov, K. (1998). Requirements for Access Control: US Healthcare Domain. In *ACM Workshop on Role-Based Access Control*, 43.

Bhatti, R., Bertino, E. & Ghafoor, A. (2005). A Trust-Based Context-Aware Access Control Model for Web-Services. *Distributed and Parallel Databases*, **18**, 83–105.

Biba, K.J. (1977). Integrity Considerations for Secure Computer Systems. Tech. rep., MITRE Corporation.

Birnhack, M.D. (2008). The EU Data Protection Directive: an Engine of a Global Regime. *Computer Law & Security Review*, **24 (6)**, 508–520.

Blaze, M. & Keromytis, A.D. (1999). The KeyNote Trust-Management System Version 2. Tech. rep., Internet Engineering Task Force RFC, this memo provides information for the Internet community.

Blobel, B. (2004). Authorisation and Access Control for Electronic Health Record Systems. *International Journal of Medical Informatics*, **73**, 251–257.

Borkin, S. (2003). The HIPAA Final Security Standards and ISO/IEC 17799. *Collection from Information Security Reading Room*.

Brennan, S. (2009). The National Programme for IT (NPfIT): Is There a Better Way? *Integrating Healthcare With Information and Communications Technology*, 95.

Bricon-Souf, N. & Newman, C. (2007). Context Awareness in Health care: A Review. *International Journal of Medical Informatics*, **76 (1)**, 2–12.

Brooke, J. (1996). SUS-A Quick and Dirty Usability Scale. *Usability Evaluation in Industry*, **189**, 4–7.

Brown, K. (2007). Exploring Claims-Based Identity. *MSDN Magazine*, **22**, 117.

Brown, P., Bovey, J. & Chen, X. (1997). Context-aware Applications: from the Laboratory to the Marketplace. *IEEE Personal Communications*, **4 (5)**, 58–64.

Brucker, A.D. & Petritsch, H. (2009). Extending Access Control Models with Break-Glass. In *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies*, 197–206, ACM.

CCBRT (2011). M-PESA Maternal Health Transport, Education & Treatment Programme. Tech. rep., Comprehensive Community Based Rehabilitation in Tanzania.

Chakraborty, S. & Ray, I. (2006). TrustBAC: Integrating Trust Relationships into the RBAC model for Access Control in Open Systems. In *Proceedings of the eleventh ACM symposium on Access control models and technologies*, 49–58, ACM.

Chandran, S.M. & Joshi, J.B. (2005). LoT-RBAC: A Location and Time-based RBAC Model. In *Web Information Systems Engineering – WISE 2005,*, 361–375, Springer.

Chen, G., Kotz, D. *et al.* (2000). Technical Report TR2000-381: A Survey of Context-Aware Mobile Computing Research. Tech. rep., Dept. of Computer Science, Dartmouth College.

Chen, P. (1976). The Entity-Relationship Model – Toward a Unified View of Data. *ACM Transactions on Database Systems (TODS)*, **1**, 9–36.

Chen, T. & Zhong, S. (2012). Emergency Access Authorization for Personally Controlled Online Health care Data. *Journal of medical systems*, **36**, 291–300.

Chou, S.C. & Wu, C.J. (2004). An Access Control Model for Workflows Offering Dynamic Features and Interoperability Ability. In *Int. Computer Symposium, Dec*, 15 – 17.

Clark, D.D. & Wilson, D.R. (1987). A Comparison of Commercial and Military Computer Security Policies. *IEEE Symposium on Security and Privacy*, 187.

Committee on Ageing Issues (2006). Report on the Ageing Population. Tech. rep., The Singaporean Government: Committee of Ageing Issues.

Covington, M., Long, W., Srinivasan, S., Dev, A., Ahamad, M. & Abowd, G. (2001). Securing Context-Aware Applications Using Environment Roles. In *Proceedings of the sixth ACM symposium on Access Control Models and Technologies*, 10–20, ACM.

Covington, M.J., Moyer, M.J. & Ahamad, M. (2000). Generalized Role-Based Access Control for Securing Future Applications. Tech. rep., Georgia Institute of Technology.

Covington, M.J., Fogla, P., Zhan, Z. & Ahamad, M. (2002). A Context-Aware Security Architecture for Emerging Applications. In *Conference Proceedings of the 18th Annual Computer Security Applications*, 249–258.

David, F. & Richard, K. (1992). Role-Based Access Controls. In *Proceedings of 15th NIST-NCSC National Computer Security Conference*, vol. 563, Baltimore, Maryland: NIST-NCSC.

Department of Health and Human Resources (2007). HIPAA Security Series. *Centers for Medicare and Medicaid Services*, **2**, 1–17.

Dey, A. (1998). Context-aware Computing: The CyberDesk Project. In *Proceedings of the AAAI 1998 Spring Symposium on Intelligent Environments*, 51–54.

Dey, A.K. (2001). Understanding and Using Context. *Personal and Ubiquitous Computing*, **5 (1)**, 4–7.

DHHR (2013). Department of health and human resources: Breaches affecting 500 or more individuals. "`http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html`", "[Online: accessed 21 April 2013]".

Downs, D.D., Rub, J.R., Kung, K.C. & Jordan, C.S. (1985). Issues in discretionary access control. In *2012 IEEE Symposium on Security and Privacy*, 208–208, IEEE Computer Society.

DuraiPandian, N., Shanmughaneethi, V. & Chellappan, C. (2006). Information Security Architecture-Context Aware Access Control Model for Educational Applications. *IJCSNS*, **6 No. 12**, 197.

Edjlali, G., Acharya, A. & Chaudhary, V. (1998). History-Based Access Control for Mobile Code. In *Proceedings of the 5th ACM conference on Computer and Communications Security*, 38–48, ACM.

EMC (2013). CyberCrime and the Healthcare Industry. Tech. rep., RSA.

European Union (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. *Official Journal L*, **281**, 0031–0050.

Evered, M. & Bögeholz, S. (2004). A Case Study in Access Control Requirements for a Health Information System. In *Proceedings of the second workshop on Australasian Information Security, Data Mining and Web Intelligence, and Software Internationalisation – Volume 32*, 53–61, Australian Computer Society, Inc.

Eysenbach, G. (2001). What is e-health? *Journal of medical Internet Research*, **3 (2)**, e20.

Federenko, I.S., Nagamine, M., Hellhammer, D.H., Wadhwa, P.D. & Wüst, S. (2004). The Heritability of Hypothalamus Pituitary Adrenal Axis Responses to Psychosocial Stress is Context Dependent. *Journal of Clinical Endocrinology & Metabolism*, **89**, 6244–6250.

Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á.O. & Toval, A. (2013). Security and Privacy in Electronic Health Records: A Systematic Literature Review. *Journal of biomedical informatics*, **46**, 541–562.

Ferraiolo, D., Cugini, J. & Kuhn, D. (1995). Role-Based Access Control: Features and Motivations. In *Proceedings of the 11th Annual Computer Security Application Conference*, 241–48, New Orleans, LA.

Ferraiolo, D., Kuhn, D. & Chandramouli, R. (2003). *Role-Based Access Control*. Artech House Publishers.

Ferraiolo, D., Kuhn, D. & Chandramouli, R. (2004). Role-Based Access Control (RBAC). *Information Systems Audit and Control Association*, **5**, 2.

Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D. & Chandramouli, R. (2001). Proposed NIST Standard for Role-Based Access Control. *ACM Transactions on Information and System Security (TISSEC)*, **4 (3)**, 224–274.

Ferreira, A., Chadwick, D., Farinha, P., Correia, R., Zao, G., Chilro, R. & Antunes, L. (2009). How to Securely Break into RBAC: the BTG-RBAC model. In *Annual Computer Security Applications Conference, 2009. ACSAC'09*, 23–31, IEEE.

Fong, P. (2004). Access Control by Tracking Shallow Execution History. In *Proceedings of the IEEE Symposium on Security and Privacy*, 43–55, IEEE.

Franqueira, N.L. & Wieringa, R. (2012). Role-Based Access Control in Retrospect. *IEEE Computer Society*, **45**, 81 – 88.

General Medical Council (2001). Good medical practice.

General Medical Council (Great Britain) (2006). *Good Medical Practice*. General Medical Council London.

Gillies, A. (2006). *The Clinician's Guide to Surviving IT*. Radcliffe Publishing.

Gish, O. (1973). Doctor auxiliaries in Tanzania. *The Lancet*, **3012 No. 7840**, 1251–1254.

Giuri, L. & Iglio, P. (1997). Role Templates for Content-Based Access Control. In *Proceedings of the second ACM workshop on Role-Based Access Control*, 153–159, ACM.

Goldschmidt, P.G. (2005). HIT and MIS: Implications of Health Information Technology and Medical Information Systems. *Communications of the ACM*, **48 (10)**, 68–74.

Gollu, K., Saroiu, S. & Wolman, A. (2007). A Social Networking-Based Access Control Scheme for Personal Content. In *Proceedings of the 21st ACM Symposium on Operating Systems Principles (SOSP07)-Work-in-Progress Session*.

Gong, L. (1989). A Secure Identity-Based Capability System. In *Proceedings of the IEEE Symposium on Security and Privacy*, 56–63, IEEE.

Goyal, V., Pandey, O., Sahai, A. & Waters, B. (2006). Attribute-Cased Encryption for Fine-Grained Access Control of Encrypted Data. In *Proceedings of the 13th ACM conference on Computer and Communications Security*, 89–98, ACM.

Graham, G.S. & Denning, P. (1972). Protection: Principles and Practice. In *Proceedings of the May 16-18, 1972, Spring Joint Computer Conference*, 417–429, ACM, New York, NY, USA.

Granger, R. *et al.* (2004). The National Programme for IT in the UK National Health Service. *World Hospitals and Health Services*, **40 (3)**, 18–22.

Grimson, J. (2001). Delivering Electronic Healthcare Record for the 21st Century. *International Journal of Medical Informatics*, **64 (2)**, 111 – 127.

Guarino, N., Masolo, C. & Vetere, G. (1999). Ontoseek: Content-Based Access to the Web. *IEEE Intelligent Systems and Their Applications*, **14 (3)**, 70–80.

Gunter, T.D. & Terry, N.P. (2005). The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions. *Journal of Medical Internet Research*, **7 (1)**.

Gupta, S.K., Mukheriee, T., Venkatasubramanian, K. & Taylor, T. (2006). Proximity Based Access Control in Smart-Emergency Departments. In *Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006*.

Hansen, F. & Oleshchuk, V. (2003). Spatial Role-Based Access Control Model for Wireless Networks. In *VTC 2003-Fall IEEE 58th Vehicular Technology Conference*, vol. 3, 2093–2097, IEEE.

Harman, L.B., Flite, C.A. & Bond, K.K.B. (2012). Electronic Health Records: Privacy, Confidentiality, and Security. *American Medical Association- Virtual Mentor*, **14**, 712–719.

Harrison, M.A., Ruzzo, W.L. & Ullman, J.D. (1976). Protection in Operating Systems. *Commununications of the ACM*, **19 (8)**, 461 – 471.

Hayes, D.R. (2014). *A Practical Guide to Computer Forensics Investigations*. Pearson Education.

Hengartner, U. & Steenkiste, P. (2004). Implementing Access Control to People Location Information. In *Proceedings of the ninth ACM Symposium on Access control Models and Technologies*, 11–20, ACM.

Henricksen, K., Indulska, J. & Rakotonirainy, A. (2002). Modeling Context Information in Pervasive Computing Systems. In *Pervasive Computing*, 79–117, Springer.

HiMSS (2014). Continuity of Care Maturity Model: Going Beyond EMRAM. "http://www.himssanalytics.org/emram/continuity.aspx", "[Online: accessed 15 April 2014]".

HIPAA (1996). Health Insurance Portability and Accountability Act of 1996. *Public Law*, **104**, 191.

HITECH (Feb 17, 2009). Health IInformation Technology for Economic and Clinical Health (HITECH) Act. *Public Law 111-5*.

HRW (2013). TOXIC TOIL: Child Labor and Mercury Exposure in Tanzanias Small-Scale Gold Mines. Tech. rep., Human Rights Watch.

Hu, V. & Scarfone, K. (2012). Guidelines for Access Control System Evaluation Metrics. Tech. Rep. NISTIR 7874, National Institute of Standards and Technology.

Hu, V., Ferraiolo, D. & Kuhn, D. (2006). *Assessment of Access Control Systems*. NIST 7316, US Department of Commerce, National Institute of Standards and Technology.

Huang, X., Wang, H., Chen, Z. & Lin, J. (2006). A Context, Rule and Role-Based Access Control Model in Enterprise Pervasive Computing Environment. In *Pervasive Computing and Applications, 2006 1st International Symposium on*, 497–502, IEEE.

IBM (2012). Tivoli Security Policy Manager. "http://www-01.ibm.com/software/tivoli/products/security-policy-mgr/", "[Online: accessed 10 January 2012]".

InfoSec (2014). Identity Management. "resources.infosecinstitute.com/identity-management/", [Online: accessed 25 January 2014].

ITNews (2013). Tanzania Creates First Cyber-Crime Laws. "http://www.itnewsafrica.com/2013/09/tanzania-creates-first-cyber-crime-laws/", "[Online: Accessed 14 April 2014]".

Jalal-Karim, A. & Balachandran, W. (2008). The National Strategies for Electronic Health Record in three Developed Countries: General status. In *INMIC 2008 – IEEE International Multitopic Conference*, 132–138, IEEE.

Jin, X., Krishnan, R. & Sandhu, R. (2012). A Unified Attribute-Based Access Control Model covering DAC, MAC and RBAC. In *Data and applications security and privacy XXVI*, 41–55, Springer.

Joshi, J., Bertino, E., Latif, U. & Ghafoor, A. (2005). A Generalized Temporal Role-Based Access Control Model. *IEEE Transactions on Knowledge and Data Engineering*, **17 (1)**, 4 – 23.

Jung, J. & Lee, J. (2007). ZigBee Device Design and Implementation for Context-aware U-healthcare System. In *ICSNC 2007 Second International Conference on Systems and Networks Communications*, 22–22, IEEE.

Kalam, A., Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C. & Trouessin, G. (2003). Organization Based Access Control. In *Proceedings of the IEEE 4th International Workshop on Policies for Distributed Systems and Networks*, 120–131, IEEE.

Karp, A., Haury, H. & Davis, M. (2009). From ABAC to ZBAC: The Evolution of Access Control Models. *Hewlett-Packard Development Company, LP*, **21**.

Kinfu, Y., Dal Poz, M.R., Mercer, H. & Evans, D.B. (2009). The Health Worker Shortage in Africa: Are Enough Physicians and Nurses Being Trained? *Bulletin of the World Health Organization*, **87 No. 3**, 225–230.

Krautsevich, L., Martinelli, F., Morisset, C. & Yautsiukhin, A. (2012). Risk-Based Auto-Delegation for Probabilistic Availability. In *Data Privacy Management and Autonomous Spontaneus Security*, 206–220, Springer.

Krishna, S. (2010). Taking Medical Records into the Digital Age: Solving Traditional System Challenges with OpenEMR. "`http://www.ibm.com/developerworks/industry/library/ind-openemr/index.html?ca=drs-`", "[Online: accessed 14 January 2014]".

Kuhn, D.R., Coyne, E.J. & Weil, T.R. (2010). Adding Attributes to Role-Based Access Control. *Computer*, **43 (6)**, 79 – 81.

Kumar, M. & Newman, R.E. (2006). STRBAC-An Approach Towards Spatio-Temporal Role-Based Access Control. In *Communication, Network, and Information Security*, 150–155.

Lærum, H., Ellingsen, G. & Faxvaag, A. (2001). Doctors' Use of Electronic Medical Records Systems in Hospitals: Cross Sectional Survey. *Bmj*, **323**, 1344–1348.

Lampson, B.W. (1971). Protection. In *Proceedings of the 5th Princeton Conference on Information Sciences and Systems*.

Lampson, B.W. (1973). "a note on the confinement problem". *Communications of the ACM*, **16 No.10**, 613–615.

Lampson, B.W. (2004). Computer Security in the Real World. *Computer*, **37 (6)**, 37 – 46.

Leonhardt, U. & Magee, J. (1997). Security Consideration for a Distributed Location Service. Tech. rep., Imperial College of Science, Technology and Medicine, London, UK.

Li, J. (2011). First Phase of Singapore National EHR Goes Live. "http://www.futuregov.asia/articles/2011/may/03/first-phase-singapore-national-ehr-goes-live/", "[Online: accessed October 2013]".

LI, L., HE, Y.Z. & FENG, D.G. (2004). A Fine-Grained Mandatory Access Control Model for XML Documents. *Journal of software*, **15**, 1528–1537.

Liu, X. (2010). *A Requirement Engineering Framework for Assessing Health care Information Systems*. Ph.D. thesis, University of Ottawa.

Lodderstedt, T., Basin, D. & Doser, J. (2002). SecureUML: A UML-based Modeling Language for Model-driven Security. In *UML 2002The Unified Modeling Language*, 426–441, Springer.

Lu, Y., Zhang, L. & Sun, J. (2008). Types for task-based access control in workflow systems. *Software, IET*, **2**, 461–473.

Madulu, N. (2012). Population Distribution and Density in Tanzania: Experiences from 2002 Population and Density Census. Tech. rep., NBS: National Bureau of Statistics.

Manzi, F., Schellenberg, J.A., Hutton, G., Wyss, K., Mbuya, C., Shirima, K., Mshinda, H., Tanner, M. & Schellenberg, D. (2012). Human Resources for Health Care Delivery in Tanzania: a Multifaceted Problem. *Hum Resour Health*, **10**, 10–1186.

McClellan, M. (2009). Duplicate Medical Records: A Survey of Twin Cities Healthcare Organizations. In *AMIA Annual Symposium Proceedings*, vol. 2009, 421, American Medical Informatics Association.

McCollum, C., Messing, J. & Notargiacomo, L. (1990). Beyond the Pale of MAC and DAC-Defining New Forms of Access Control. In *IEEE Computer Society Symposium on Research in Security and PrivacyProceedings*, 190–200, IEEE.

MCDGC (2012). Tanzania National Strategy for Gender Development. Tech. rep., Ministry of Community Development , Gender and Children.

Mercuri, R. (2004). The HIPAA-potamus in Health care Data Security. *Communications of the ACM*, **47 (7)**, 25 – 28.

Mhagama, H. (2013). Tanzania: Marine Accidents Leave 245 Dead. "http://allafrica.com/stories/201307250436.html", "[Online: accessed 17 March 2014]".

Microsoft (2005). Authorization Manager. "http://technet.microsoft.com/en-us/library/cc757023(v=ws.10).aspx", "[online: accessed 10 January 2012]".

Miguel-Garcia, A.I., Favela, J. & Victor, M. (2003). Context-Aware Mobile Communication in Hospitals. *Computer*, **36 (9)**, 38 – 46.

Miller, R. & Sim, I. (2004). Physicians use of Electronic Medical Records: Barriers and Solutions. *Health Affairs*, **23 (2)**, 116–126.

Mills, A. (1998). Health Policy Reforms and their Impact on the Practice of Traditional Medicine. *British Medical Bulletin*, **54 (2)**, 503 – 513.

Ministry of Health (2012). Speech by Dr Amy Khor, Minister of State for Health - Healthcare Scholarship Award Ceremony. "http://www.moh.gov.sg/content/

moh_web/home/pressRoom/speeches_d/2012/speech-Dr-Amy-Khor", "[Online: accessed 13 December 2013]".

Ministry of Home Affairs (2012). Road Accidents in Tanzania. "www.moha.go.tz", "[Online: accessed 17 April 2014]".

Minsky, N.H. & Lockman, A.D. (1985). Ensuring integrity by Adding Obligations to Privileges. In *Proceedings of the 8th international conference on Software engineering*, 92–102, IEEE Computer Society Press.

Mkony, C. (2010). Experience with Training of Medical Professionals in Tanzania. In *Proceedings of the 43rd Annual General Meeting and the 45th Annivesary* , Medical Association of Tanzania.

MoHSW (1990). The United Republic of Tanzania Ministry of Health: National Health Policy. Tech. rep., Ministry of Health and Social Welfare, from Website.

MoHSW (2001). Tanzania Fistula Survey 2001. Tech. rep., Ministry of Health and Social Welfare.

MoHSW (2003). The United Republic of Tanzania Ministry of Health: National Health Policy. Tech. rep., Ministry of Health and Social Welfare, from Website.

MoHSW (2007). The United Republic of Tanzania Ministry of Health and Social Welfare: National Health Policy. Tech. rep., Ministry of Health and Social Welfare, from Website.

MoHSW (2008a). Human Resource For Health Strategic Plan 2008 2013. Tech. rep., Ministry of Health and Social Welfare, website.

MoHSW (2008b). The National Road Map Strategic Plan to Accelerate Reduction of Maternal, Newborn and Child Deaths in Tanzania 2008-2015. Tech. rep., Ministry of Health and Social Welfare.

MoHSW (2009). Health Sector Strategic Plan III July 2009 - June 2015: Partership for Delivering the MDGs. Tech. rep., Ministry of Health and Social Welfare.

MoHSW (2012). Taarifa ya Magonjwa ya Wiki, Wiki ya 39. Tech. rep., Ministry of Health and Social Welfare.

MoHSW (2013). Human Resources for Health Country Profile 2012/2013. Tech. rep., Ministry of Health and Social Welfare.

MoHSW (2013a). National Costed Plan of Action for Most Vulnerable Children (MVC) (NCPA II). Tech. rep., Ministry of Health and Social Welfare: Department of Social Welfare.

MoHSW (2013b). Summary and Analysis of the Comprehensive Council Health Plans 2013/2014. Tech. rep., Ministry of Health and Social Welfare and Prime Minister's Office Regional Administration and Local Government.

MoHSW (2013c). Tanzania National e-Health Strategy 2012-2018. Tech. rep., Ministry of Health and Social Welfare.

MoHSW (2014). Taarifa ya Magonjwa ya Wiki, Wiki ya 7. Tech. rep., Ministry of Health and Social Welfare.

Monitor (2008). Guidance for NHS Foundation Trusts on Cooperating with the National Programme for Information Technology. Tech. rep., Monitor: The Independent Regulator of NHS Foundation Trusts.

Motta, G.H. & Furuie, S.S. (2003). A contextual role-based access control authorization model for electronic patient record. *Information Technology in Biomedicine, IEEE Transactions on*, **7**, 202–207.

Mukherjee, A. & McGinnis, J. (2007). E-healthcare: an Analysis of Key Themes in Research. *International Journal of Pharmaceutical and Healthcare Marketing*, **1 (4)**, 349 – 363.

Munishi, G. (1997). Private Health Care in Tanzania: Private Health Sector Growth Following Liberalization in Tanzania. *Report on Work in Progress with Support from the International Health Policy Programme. Dar es Salaam: University of Dar es Salaam and the International Health Policy Programme*.

Nanda, A. & Burleson, D.K. (2003). *Oracle Privacy Security Auditing*. Rampant.

National Audit Office (2009). National Audit Office Department of Health (2006) The National Programme for IT in the NHS Second Report of Session 200809. Tech. rep., House of Commons Public Accounts Committee.

National Bureau of Statistics (2009). Basic Facts and Figures on Human Settlements: Tanzania Mainland 2009. Tech. rep., National Bureau of Statistics.

National Bureau of Statistics (2011). Tanzania Demographic and Health Survey. Tech. rep., National Bureau of Statistics.

National Bureau of Statistics (2013). Population Distribution by Administrative Units: Key Findings from the 2012 Population and Housing Census. Tech. rep., National Bureau of Statistics-Tanzania.

National Center for Biotechnology Information (2012). Radiology Information Systems, Hospital Information Systems, Clinical Information Systems, Pharmacy Information Systems, Operating Room Information Systems. "`http://www.ncbi.nlm.nih.gov/mesh?term=InformationSystems`", "[Online: accessed 14 January 2013]".

National E-health Transition Authority (2011). NEHTA Blueprint Version 2.0. Tech. rep., National E-Health Transition Authority.

National Electrical Manufacturers Association, European Coordination Committee of the Radiological and Electromedical Industry & Japan Industries Association of Radiological Systems (2004). Break-Glass - An Approach to Granting Emergency Access to Healthcare Systems. Tech. rep., Joint NEMA (National Electrical Manufacturers Association – USA), COCIR (European Coordination Committee of the Radiological and Electromedical Industry) and JIRA (Japan Industries Association of Radiological Systems) Security and Privacy Committee, from Website.

NBS (2010). Tanzania in Figures. Tech. rep., National Bureau of Statistics, Ministry of Finance, Tanzania.

NBS (2012a). Population and Housing Census Counts. "http://www.nbs.go.tz/sensa2012/", "[Online: accessed 13 January 2013]".

NBS (2012b). Statistical Abstract 2012. Tech. rep., National Bureau of Statistics.

NBS (2013). Tanzania in Figures 2012. Tech. rep., National Bureau of Statistics.

Nehemiah, L. (2014). Towards ehr interoperability in tanzania hospitals: Issues, challenges and opportunities. *International Journal of Computer Science, Engineering and Applications arXiv:1410.2205*, **4 No. 4**, 29 – 36.

NHS (2012). Spine. "http://www.connectingforhealth.nhs.uk/systemsandservices/spine", "[Online: accesed on 31 January 2013]".

Ni, Q., Trombetta, A., Bertino, E. & Lobo, J. (2007). Privacy-aware role based access control. In *Proceedings of the 12th ACM symposium on Access control models and technologies*, SACMAT '07, 41–50, ACM, New York, NY, USA.

Oh, S. & Park, S. (2003). Task-Role-Based Access Control Model. *Information Systems*, **28**, 533–562.

Omary, Z., Mtenzi, F. & Wu, B. (2009). How does Politics affect Electronic Healthcare Adoption. In *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, 1–8, IEEE.

Omary, Z., Mtenzi, F. & Wu, B. (2011). *Context and Access Control for Healthcare*, chap. 3, 21–31. MASAUM NETWORK.

Oreku, G., Mtenzi, F. & Al-Dahoud, A. (2011). "The Prospects and Barriers of E-Commerce Implementations in Tanzania". In *ICIT 2011 The 5th International Conference on Information Technology*.

Osborn, S., Sandhu, R. & Munawer, Q. (2000). Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies. *ACM Transactions on Information and System Security (TISSEC)*, **3 (2)**, 85 – 106.

Othman, H., Mukandala, R., Makaramba, R. & Tidemand, P. (2003). Local Governance in Zanzibar. Tech. rep., Revolutionary Government of Zanzibar.

Ouchi, K., Suzuki, T. *et al.* (2002). LifeMinder: a Wearable Healthcare Support System using User's Context. In *Proceedings: 22nd International Conference on Distributed Computing Systems Workshops*, 791–792, IEEE.

Parliament (1971). United Republic of Tanzania, Tanzania Law of Marriage Act. Tech. rep., Parliament, United Republic of Tanzania.

Parliament (2009). House of Commons Public Accounts Committee and others The national Programme for IT in the NHS: Progress Since 2006. Tech. rep., House of Commons.

Parliament (2011). The National Programme for IT in the NHS: an Update on the Delivery of Detailed Care Records Systems, Forty-Fifth Report of Session 2010-12. Tech. rep., House of Commons- Committee of Public Accounts.

Paul, R.A. (2007). Proposition for E-DoD: An Overall Plan for Network Centric Operation. In *Seventh International Conference on Quality Software - QSIC'07*.

Paulson, P. & Snyder, K. (2005). E-healthcare: Strategies to Consider. *International Journal of Electronic Healthcare*, **1 (4)**, 442–452.

Pervaiz, Z., Samuel, A., Ferraiolo, D., Gavrila, S. & Ghafoor, A. (2010). Access Control for Healthcare using Policy Machine, [Available in Citeseer].

Pigeot, C.E., Gripay, Y., Scuturici, M. & Pierson, J.M. (2007). Context-sensitive security framework for pervasive environments. In *Universal Multiservice Networks, 2007. ECUMN'07. Fourth European Conference on*, 391–400, IEEE.

Pimlott, A. & Kiselyov, O. (2006). Soutei, a Logic-Based Trust-Management System. *Functional and Logic Programming*, –, 130–145.

Prime Minister's Office RALG (2012). Regional Administration. "`http://www.pmoralg.go.tz/regional_profiles/index.php`", "[Online: accessed 19 June 2012]".

Proctor, N. & Wong, R. (1989). The Security Policy of the Secure Distributed Operating System Prototype. *Fifth Annual Computer Security Applications Conference*, 95–102.

Ray, I. & Kumar, M. (2006). Towards a Location-Based Mandatory Access Control Model. *Computers & Security*, **25 (1)**, 36–44.

Ray, I., Kumar, M. & Yu, L. (2006). LRBAC: A Location-Aware Role-Based Access Control Model. *Information Systems Security*, 147–161.

Rice, D. (2007). *Geekonomics: The Real Cost of Insecure Software*. Pearson Technology Group Canada.

Rindfleisch, T.C. (1997). Privacy, Information Technology, and Health care. *Communications of the ACM*, **40**, 92–100.

Roach, W.H. (2006). *Medical Records and the Law*. Jones & Bartlett Learning.

Rostad, L. & Edsberg, O. (2006). A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs. In *Computer Security Applications Conference, 2006. ACSAC'06. 22nd Annual*, 175–186, IEEE.

Ryan, N., Pascoe, J. & Morse, D. (1998). Enhanced Reality Fieldwork: the Context-Aware Archaeological Assistant. In *Computer Applications in Archaeology*, Tempus Reparatum.

Salber, D., Dey, A.K. & Abowd, G.D. (1999). The Context Toolkit: Aiding the Development of Context-Enabled Applications. In *Proceedings of the SIGCHI conference on Human factors in computing systems: the CHI is the limit*, 434–441, ACM.

Samarati, P. & de Vimercati, S. (2001). Access Control: Policies, Models and Mechanisms. *Foundations of Security Analysis and Design*, 137 – 196.

Sampemane, G., Naldurg, P. & Campbell, R.H. (2002). Access Control for Active Spaces. In *Proceedings 18th Annual Computer Security Applications Conference*, 343–352, IEEE.

Sandhu, R. (1993). Lattice-Based Access Control Models. *Computer*, **26 (11)**, 9 –19.

Sandhu, R. (1996a). Access Control: The Neglected Frontier. In *Information Security and Privacy*, 219–227, Springer.

Sandhu, R. (1996b). Rationale for the RBAC96 Family of Access Control Models. In *Proceedings of the First ACM Workshop on Role-Based Access Control*, 9, ACM.

Sandhu, R. & Park, J. (2003). Usage control: A vision for next generation access control. In *Computer network security*, 17–31, Springer.

Sandhu, R. & Samarati, P. (1994). Access Control: Principle and Practice. *IEEE Communications Magazine*, **32 (9)**, 40–48.

Sandhu, R. & Samarati, P. (1996). Authentication, Access Control, and Audit. *ACM Computing Surveys (CSUR)*, **28 (1)**, 241–243.

Sandhu, R., Coyne, E., Feinstein, H. & Youman, C. (1996). Role-Based Access Control Models. *Computer*, **29 (2)**, 38–47.

Sandhu, R., Ferraiolo, D. & Kuhn, R. (2000). The NIST Model for Role-Based Access Control: Towards a Unified Standard. In *Proceedings of the Fifth ACM workshop on Role-Based Access Control*, 47–63, Citeseer.

SARUA (2011). Tanzania Data Profile 2012. Tech. rep., Southern African Regional Universities Association.

Satyanarayanan, M. (2001). Pervasive Computing: Vision and Challenges. *IEEE Personal Communications*, **8 (4)**, 10 – 17.

Schilit, B. & Theimer, M. (1994). Disseminating Active Map Information to Mobile Hosts. *IEEE Network*, **8 (5)**, 22 – 32.

Schilit, B., Adams, N. & Want, R. (1994). Context-aware Computing Applications. In *First Workshop on Mobile Computing Systems and Applications WMCSA'94*, 85–90, IEEE.

Schmidt, A., Beigl, M. & Gellersen, H.W. (1999). There is more to Context than Location. *Computers & Graphics*, **23 (6)**, 893 – 901.

Schoenberg, R. & Safran, C. (2000). Internet Based Repository of Medical Records that Retains Patient Confidentiality. *BMJ*, **321 (7270)**, 1199 – 1203.

Sharma, S.K., Xu, H., Wickramasinghe, N. & Ahmed, N. (2006). Electronic healthcare: Issues and challenges. *International journal of electronic healthcare*, **2**, 50–65.

Shekelle, P., Morton, S. & Keeler, E. (2006). *AHRQ Evidence Reports*, chap. Costs and Benefits of Health Information Technology, 132. Agency for Healthcare Research and Quality (US).

Shen, H. & Hong, F. (2006). An Attribute-Based Access Control Model for Web Services. In *Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT'06. Seventh International Conference on*, 74–79, IEEE.

Smith, M., Madon, S., Anifalaje, A., Lazarro-Malecela, M. & Michael, E. (2008). Integrated Health Information Systems in Tanzania: Experence and Challenges. *Electronic Journal of Information Systems in Developing Countries*, **33**, 1 – 21.

Soffa, M.L. (2007). Developing a Testing Framework for Security. *ABOUT THIS REPORT*, –, 6.

Sommerville, A. & Horner, J.S. (1993). *Medical Ethics Today: its Practice and Philosophy*. BMJ Publishing Group.

Starr, P. (1996). The Signing of the Kennedy-Kassebaum Bill. "`https://www.princeton.edu/~starr/articles/signing.html`", "[Online: accessed 14 April 2014]".

Stroetmann, K., Jones, T., Dobrev, A. & Stroetmann, V. (2006). eHealth is Worth it: The Economic Benefits of Implemented eHealth Solutions at Ten European Sites. *eHealth Impact*, –, –.

Tan, J. (2005). *E-health Care Information Systems: an Introduction for Students and Professionals*. Jossey-Bass.

Tanzania Food and Nutrition Centre (2013). Severe Acute Malnutrition. "http://www.tfnc.or.tz/eng/focus/pem.htm", "[Online: accessed 17 April 2014]".

Tanzania Online (2012). Discussion Paper on the Introduction of a Legal Framework for Electronic Commerce in Tanzania. "www.tzonline.org", "[online, accessed 01-June-2013]".

TCSEC (1985). Trusted Computer Security Evaluation Criteria. Tech. Rep. DoD 5200.28-STD, Department of Defense.

TCU (2012). Admissions Guidebook for Higher Education Institutions in Tanzania. Tech. rep., Tanzania Commission for Universities.

TechTarget (2005). Definition of Granularity taken from "whatis.com". "http://whatis.techtarget.com/definition/granularity", "[Online, accessed 01-June-2014]".

TechTarget (2006). Definition of Scalability taken from "searchdatacenter". "http://searchdatacenter.techtarget.com/definition/scalability", "[Online, accessed 01-June-2014]".

Tett, T. (2010). NPFIT-FNT-TO-TAR-0043.06 General Practice IT Infrastructure Specification. Tech. rep., National Health Service (NHS).

Thomas, R. (1997). Team-Based Access Control (TMAC): a Primitive for Applying Role-Based Access Controls in Collaborative Environments. In *Proceedings of the second ACM workshop on Role-based access control*, 13–19, ACM.

Thomas, R. & Sandhu, R. (1993). Towards a Task-based Paradigm for Flexible and Adaptable Access Control in Distributed Applications. In *Proceedings on the 1992-1993 Workshop on New Security Paradigms*, 138–142, ACM.

Thomas, R. & Sandhu, R. (1998). Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management. *Database Security*, **11**, 166–181.

Toninelli, A., Montanari, R. & Corradi, A. (2009). Enabling secure service discovery in mobile healthcare enterprise networks. *Wireless Communications, IEEE*, **16**, 24–32.

Tran, H., Hitchens, M., Varadharajan, V. & Watters, P. (2005). A Trust Based Access Control Framework for P2P File-Sharing Systems. In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences HICSS'05*, 302c–302c, IEEE.

Trotter, F. (2012). Who owns Patient Data? "`http://strata.oreilly.com/2012/06/patient-data-ownership-access.html`", "[Online: accessed 14 March 2014]".

United Nations DESA (2012). World Population Prospects The 2012 Revision Volume I: Comprehensive Tables. Tech. rep., United Nations Department of Economic and Social Affairs: Population Division.

Varshney, U. (2007). Pervasive Healthcare and Wireless Health Monitoring. *Mobile Networks and Applications*, **12 (2 − 3)**, 113–127.

Wan, K. (2009). A Brief History of Context. *International Journal of Computer Science Issues, IJCSI*, **6 (2)**.

Wang, H., Sheng, B. & Li, Q. (2006). Elliptic Curve Cryptography-Based Access Control in Sensor Networks. *International Journal of Security and Networks*, **1 (3)**, 127 – 137.

Winograd, T. (2001). Architectures for Context. *Human-Computer Interaction*, **16 (2)**, 401 – 419.

Wood, A., Stankovic, J., Virone, G., Selavo, L., He, Z., Cao, Q., Doan, T., Wu, Y., Fang, L. & Stoleru, R. (2008). Context-Awareware Wireless Sensor Networks for Assisted Living and Residential Monitoring. *IEEE Network*, **22 (4)**, 26 – 33.

World Bank (2014). Physicians (per 1000 people) World Health Organisation's Global Health Workforce Statistics, OECD, Supplemented by Country Data. `data.worldbank.org/indicator/SH.MED.PHYS.ZS`, "[Online: accessed 11-June-2015]".

World Bank (2015). Physicians (per 1000 people). Online.

World Health Organisation (2005). The Impact of Chronic Disease in China. "`http://www.who.int/chp/chronic_disease_report/media/china.pdf`", "[Online: accessed 08 January 2013]".

World Health Organisation (2008). Management of Health Facilities: Referral Systems. urlhttp://www.who.int/management/facility/referral/en.

World Health Organisation (2011). Global Status Report on Noncommunicable Diseases. Tech. rep., World Health Organisation (WHO).

World Health Organisation (2012a). About Ageing and Life-Course. "http://www.who.int/ageing/about/ageing_life_course/en/index.html", "[Online: accessed 08 January 2013]".

World Health Organisation (2012b). Disability and Health. Tech. rep., World Health Organisation (WHO), from Website.

World Health Organisation (2012c). United Republic of Tanzania: Health Profile. urlhttp://www.who.int/countries/tza/en/, "[Online: accessed 11 January 2013]".

World Health Organisation (2013a). A Universal Truth: No Health Without A Workforce. Tech. rep., World Health Organisation.

World Health Organisation (2013b). Diasbility and Health. Tech. rep., World Health Organisation.

Wyatt, J. & Sullivan, F. (2005). eHealth and the Future: Promise or Peril? *BMJ*, **331 (7529)**, 1391 – 1393.

Wyatt, J.C. & Wright, P. (1998). Design should help Use of Patients' Data. *The Lancet*, **352**, 1375–1378.

Yuan, E. & Tong, J. (2005). Attributed Based Access Control (ABAC) for Web Services. In *Proceedings IEEE International Conference on Web Services ICWS 2005*, Ieee.

Zhang, D., Yu, Z. & Chin, C.Y. (2005a). Context-Aware Infrastructure for Personalized Healthcare. *Studies in Health Technology and Informatics*, **117**, 154 – 163.

Zhang, G. & Parashar, M. (2003). Dynamic Context-Aware Access Control for Grid Applications. In *Proceedings of the. Fourth International Grid Computing Workshop*, 101–108.

Zhang, X., Li, Y. & Nalla, D. (2005b). An Attribute-Based Access Matrix Model. In *Proceedings of the 2005 ACM symposium on Applied Computing*, 359–363, ACM.

Zhao, G., Chadwick, D. & Otenko, S. (2007). Obligations for Role Based Access Control. In *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*, vol. 1, 424–431, IEEE.

Appendices A

Research Ethical Clearance

A.1 NIMR

THE UNITED REPUBLIC OF
TANZANIA

National Institute for Medical Research
P.O. Box 9653
Dar es Salaam
Tel: 255 22 2121400/390
Fax: 255 22 2121380/2121360
E-mail: headquarters@nimr.or.tz
NIMR/HQ/R.8a/Vol. IX/1015

Ministry of Health and Social Welfare
P.O. Box 9083
Dar es Salaam
Tel: 255 22 2120262-7
Fax: 255 22 2110986

29th September 2010

Ms Zanifa Omary
Institute of Finance Management
Shaaban Robert Street
P O Box 3918,
DAR ES SALAAM

CLEARANCE CERTIFICATE FOR CONDUCTING MEDICAL RESEARCH IN TANZANIA

This is to certify that the research entitled: Context-Aware Access Control Framework for Securing Patients Healthcare Information in a Collaborative Healthcare Environment in Tanzania, (Omary Z *et al)*, has been granted ethics clearance to be conducted in Tanzania.
The Principal Investigator of the study must ensure that the following conditions are fulfilled:

1. Annual Progress report is submitted to the Ministry of Health and the National Institute for Medical Research, Regional and District Medical Officers.
2. Permission to publish the results is obtained from National Institute for Medical Research.
3. Copies of final publications are made available to the Ministry of Health & Social Welfare and the National Institute for Medical Research.
4. Any researcher, who contravenes or fails to comply with these conditions, shall be guilty of an offence and shall be liable on conviction to a fine. NIMR Act No. 23 of 1979, PART III Section 10(2).
5. Approval is for one year: 29th September 2010 to 28th September 2011.

Name: Dr Mwelecele N Malecela
Signature
ACTING CHAIRPERSON
MEDICAL RESEARCH
COORDINATING COMMITTEE

Name: Dr Deo M Mtasiwa
Signature
CHIEF MEDICAL OFFICER
MINISTRY OF HEALTH, SOCIAL
WELFARE

CC: RMO
DMO

A.2 MNH

MUHIMBILI NATIONAL HOSPITAL

Cables: "MUHIMBILI"
Telephones: 255-22-2151599
255-22-2151369
FAX: 255-22-2150234
Email: dcs@mnh.or.tz
Web: www.mnh.or.tz

Postal Address:
P.O. Box 65000
Muhimbili
DAR ES SALAAM
Tanzania

August 19, 2010

TO WHOM IT MAY CONCERN,
MUHIMBILI NATIONAL HOSPITAL

RE: RESEARCH CLEARANCE NO.10 OF 2010/2011

Name of Researcher:	**ZANIFA OMARY**
Research Title:	**CONTEXT-AWARE ACCESS CONTROL FRAMEWORK FOR SECURING PATIENT'S HEALTHCARE INFORMATION IN A COLLABORATIVE ENVIRONMENT IN TANZANIA**
Subjects	**MNH HEALTH INFORMATION SYSTEM: NO PATIENT DATA IS REQUIRED**
Time	**AUGUST 2010 – SEPTEMBER 2011**

The above named has been allowed to conduct the stated research at MNH.

Please accord her/her assistants the necessary assistance/ cooperation.

Sincerely,

Prof. Andrew B.M. Swai
DIRECTOR OF MEDICAL SERVICES

A.3 Ilala Municipal Council

ILALA MUNICIPAL COUNCIL

ALL COMMUNICATIONS TO BE ADDRESSED TO THE MUNICIPAL DIRECTOR

P.O. BOX 20950
PHONE NO: 2128800
2128805
FAX NO. 2121486

MUNICIPAL OFFICE
ILALA

19/12/2010

Ref: IMC/MED/F.6/1 Vol.L.II /....

Medical Officer in Charge
Mnazi Mmoja Health Centre/Amana/Buguruni
Ilala Municipality

RE: PERMISSION TO CONDUCT A STUDY AT YOUR FACILITY.

Please refer to the heading above.

Zanifa Omary is the PhD Student- School of Computing Dublin Institute of Technology is requesting to conduct a study on (Context-Aware Access Control Framework for Securing Patient's Healthcare Information in Collaborative Healthcare environment in Tanzania) at your Health Facility.

The study is a part of her academic fulfilment in PhD Programme. I attach a copy of Clearance Certificate for Conducting Medical Research in Tanzania for your references

For this reason I hereby request your assistance in the whole period of her study at your facility.

District Health Planning Coordinator
For: **MMOH -ILALA**
Copy: **PhD- Student**

Appendices B

Survey in Tanzania

Enhancing Access to Sensitive Electronic Health Records in Tanzania

For any correspondence, please do not hesitate to contact

Ms. Zanifa Omary

School of Computing

Dublin Institute of Technology

Kevin Street, Dublin 8, Dublin, Ireland Republic

Zanifa.Omary@dit.ie

Mobile: +353 86 344 6592

SECTION I: DEMOGRAPHIC INFORMATION

1. Professional category

   ☐ Consultant

   ☐ Doctor

☐ Nurse

☐ Pharmacist

☐ System Administrator

☐ Other, *specify*

2. Department

3. Type of healthcare institution (*please tick only one*)

☐Government-owned

☐Parastatal

☐Faith-based

☐Private

4. It is a

☐Referral hospital

☐Regional hospital

☐District hospital

☐Health centre

☐Dispensary

5. Which region does your healthcare facility serve?

☐Arusha

☐Dar es Salaam

☐Kilimanjaro

☐Mbeya

☐Mwanza

☐Other, *specify*

6. For the purpose of controlling responses, please provide the name of the institution that you are affiliated with

7. Experience (in years)

☐0-5

☐6-10

☐11-15

☐16-20

☐More than 20

8. Academic proficiency

☐Bachelor Degree

☐Masters

☐PhD

☐Other, *specify*

9. Gender

☐Female

☐Male

SECTION II: ELECTRONIC HEALTHCARE

10. Do you understand what electronic healthcare is?

☐Yes

☐No

11. How do you rate your level of understanding of electronic healthcare?

☐Excellent

☐Very Good

☐Good

☐Fair

☐Poor

12. Do you have electronic healthcare information system in your organisation?

☐Yes

☐No, *go to question 16*

13. Which health care information system is being used in your organisation? (*please tick all appropriate systems available*)

☐Electronic Medical Record System

☐Laboratory Information System

☐Radiology Information system

☐Pharmacy Information System

☐Picture Archiving and Communication System (PACS)

☐Other, *specify*

14. What triggered the adoption and use of electronic healthcare information system(s) in your organisation? *(Choose appropriate)*

☐Better coordinated care

☐Reducing patients waiting time

☐Less paperwork

☐Other, *specify*

15. Do y
syste

☐Yes

☐No

16. What are the challenges facing Tanzania healthcare system that could benefit from the adoption of electronic medical record systems?

☐Lack of enough workforces

☐Health inequalities

☐Low productivity of staff, who are present

☐Other, *specify*

SECTION III: ELECTRONIC MEDICAL RECORD

17. Have you ever used either electronic medical record or electronic health record system?

☐Yes

☐No, *go to question 21*

18. For how long have you been using these systems?

☐0-3 years

☐4-6 years

☐7-10 years

☐Other , *specify*

19. What are the main reasons of using electronic medical record system in your organisation?

☐Data input

☐Decision support

☐Prescription

☐Emergency data access

☐Don't know

☐Other, *specify*

20. Do you think medical records processed by electronic medical record systems are

☐Indispensable

☐Important for my work

☐Not useful

☐Other, specify

21. What do you think are the problems of electronic medical record systems?

☐It is a waste of time

☐They affect patient/doctor relationship

☐They are not secure

☐They require education

☐Other, *specify*

SECTION IV: ACCESS CONTROL

22. What mechanism do you normally use to access electronic medical records?

☐Login/password

☐Biometrics

☐Using someone else's credentials

☐Other, *specify*

23. If you use login/password to access medical records, what are their associated challenges? (*choose all appropriate reasons*)

☐You may forget it, many times

☐You can share your password

☐You can access records easily

☐Other, *specify*

24. Do you think access to electronic medical records must be controlled using roles (such as nurse, doctor etc.) established in the organisation?

☐Yes,

☐Only roles are enough, *go to question 26*

☐Role with other information, *go to question 25*

☐No

25. In addition to roles, what other information do you consider necessary for controlling access to electronic medical record?

☐Location

☐Time

☐Purpose of access

☐Other, *specify*

26. Do you think patients should be given access to their medical records?

☐Yes

☐No, *explain why*

27. Should there be any mechanisms to allow healthcare professional to access patient's medical records in case of an emergency?

☐Yes

☐Everybody should have access

☐Only certain roles should be granted access

☐Depending on the emergency

☐No

SECTION V: ACCESS TO MEDICAL RECORDS: SITUATIONS

This section intends to collect situations involved in access to medical records. The situations collected may include the following information

- Who (in terms of role) requests to access medical records?
- What type of data is disclosed?
- What type of task is carried out?
- Any other conditions involved such as location, time etc.

Sample situation: *As* ***a registered nurse****, I am allowed* ***to view diagnosis of inpatient*** *if he is* ***located in the pediatrics unit and my workspace is the pediatrics unit***

28. Describe situations involving your daily access to sensitive medical data

29. **Unusual data disclosure situations:**

i. Have you ever been involved in a situation where patient's data, which seems to be not relevant to a certain role at the beginning, become relevant under certain circumstances?

☐Yes

☐No

ii. Have you ever been involved in unusual situations that were differently conducted in comparison to regular routines?

☐Yes, *go to iii*

☐No

iii. If **Yes**, list those situations here

Thank you in Advance!

C.1 role-based

1. Alice, with a role consultant surgeon, requested to read medical records of patient
2. A medical doctor named Bob requested to access electronic health records of patient
3. A receptionist named Anne requested to read medical records of a patient
4. A specialist consultant requested to access billing information of a patient
5. A system administrator requested to delete medical records of a patient
6. A senior system administrator sent an access request to create medical records of a patient
7. A surgeon doctor requested to access medical records of a patient who is scheduled for an open heart surgery
8. A medical doctor requested to access medical records of an out patient
9. A specialist consultant requested to access billing information of a patient.
10. A nurse working in a diabetic ward in a public clinic within a hospital requested to access medical records of a patient who is currently not receiving any treatment from the hospital.
11. A registered nurse requested to create medical records of a newborn baby found in a dumping site
12. A clinical assistant requested to read medical records of a patient who is a primary school student
13. A social worker requested to access medical records of a newborn baby
14. A receptionist requested to read billing information of a patient from the front desk
15. A system administrator requested to delete medical records of a patient from system administrators' office.
16. An enrolled nurse sent an access request to read medical records of a patient
17. A registered nurse requested to create medical records of a newborn baby
18. A clinical assistant requested to read medical records of a patient suffering from third degree burns from a house fire
19. A cardiologist named Bob attempted three times to access medical records of a patient from the cardiology department.
20. A surgeon doctor requested to access medical records of a patient who is scheduled for an open heart surgery
21. A registered nurse requested to access medical records of a woman in critical condition
22. An intern medical doctor is requesting to access medical records of a patient

C.2 context-based

1. On a night shift, a surgeon consultant has requested to access medical records of a patient with albinism whose limbs has been amputated non-surgically

2. A surgeon consultant requested to access medical records of a patient injured from bomb explosion. An access request was sent from an operating room during a day shift.
3. A medical doctor requested to access medical records of a patient from an Intensive Care Unit (ICU) while attending an emergency situation on an unidentified individual who was brought in by the police officer.
4. As a result of wrong permissions specified in a system that restricted access to medical records of a patient from a ward, a medical doctor requested to access electronic health records of a patient from the front desk.
5. A cardiologist named Bob attempted three times to access medical records of a patient from the cardiology department.
6. A surgeon doctor requested to access medical records of a patient who is scheduled for an open heart surgery as a result of a cardiogenic embolic stroke.
7. A medical doctor requested to access medical records of an out patient from his office during a night shift.
8. A specialist consultant requested to access billing information of a patient from a ward.
9. A specialist doctor requested to read patient's personal information from the front desk of a hospital during a night shift.
10. A receptionist requested to access medical records of a patient with no specific reason. An access request was sent from the front desk at 5:40 p.m.
11. While working in a night shift in a physiotherapy department, a medical doctor requested to read billing records of a patient suffering from diabetes mellitus.
12. A clinical assistant is requesting to read medical records of a patient suffering from third degree burns from a house fire. An access request was sent from the same ward where the patient is located, during a day shift
13. In a district hospital, a registered nurse requested to access medical records of a woman who was stabbed by her husband. An access request was sent from the ICU during a night shift.
14. In a dispensary, a nurse requested to access medical records of a patient injured from a bomb explosion.
15. A nurse working in a diabetic ward in a public clinic in a hospital requested to access billing information of a patient suffering from diabetes mellitus
16. A nurse working in a diabetic ward in a public clinic within a hospital requested to access medical records of a patient who is currently not receiving any treatment from the hospital.
17. A registered nurse requested to create medical records of a newborn baby found in a dumping site, and was brought to the hospital by a police officer during a day shift.
18. A clinical assistant requested to read medical records of a primary school girl who was abused by unidentified individual while walking home from school. This access request was sent during a night shift.

19. A social worker requested to access medical records of a newborn baby who was brought in the hospital by police officers after being found in a dumping site.
20. A social worker requested to read medical records of a child who suffers from malnutrition. Such a request was sent from the childrens' ward during a day shift.
21. A social worker requested to access medical records of a child suffering from both malnutrition and child abuse from childrens' ward at 8:30 p.m. The child who has a disability was deliberately starved by his parents.
22. A social worker sent two access requests from outside the hospital. One access request was sent during the day and another during the night shift, and the social worker was requesting to access medical records of a three years old boy who has broken ribs while he is at his mother's care.
23. A receptionist requested to read billing information of a patient from the front desk during a day shift
24. A pharmacist requested to read billing information of a patient from the pharmacy, which is part of a hospital, during a night shift
25. A pharmacist sent an access request from a front desk to read medical records of a twelve years old girl who is pregnant, and is having complications during labour and delivery.
26. An enrolled nurse sent an access request to read medical records of a patient from the ward during a night shift [that is, 18:00 - 6:00 p.m.]
27. A system administrator is requesting to delete medical records of a patient from system administrators' office.
28. A senior system administrator sent an access request to create medical records of a new patient. The records to be created are for a woman who was assaulted by her husband in gender-based violence situation. The request was sent during a day shift

Health-related Contexts

1. **Ministry of Community Development, Gender and Children**

   (a) Widow Cleansing and Inheritance

   Widow cleansing and inheritance is a practice performed to women of certain tribes in Tanzania after the death of their husbands. Typically, a widowed woman is expected to have unprotected sex with men from her husband's family which will then allow her to keep her assets. This act introduces women to assaults and in worst case, they might end up getting infected with sexually transmitted diseases. As reported by the Human Right Watch on Domestic Abuse and HIV infection, widow inheritance goes hand in hand with diseases (MCDGC, 2012).

   (b) Marriage by Abduction

   This act involves unlawful carrying away of a girl or young woman, usually by force, for the intention of getting married. Typically an abductor arranges a group of intimate friends and relatives to kidnap a girl or young woman (in rare cases) without informing her family, relatives or friends. And in some cases, abduction is followed by rape. The public blames the Tanzania education system for abductions in young girls since it does not provide enough security for them. In rural areas, for instance, school children walk long distances to and from school, which exposes them to risks of rape or abduction into marriages.

   (c) Pregnancy in Adolescent Girls

   Tanzania laws, especially the Tanzania Law Marriage Act, do not criminalise anti-girl practices such as early marriage (Parliament, 1971). In some parts of the country, it is common for girls as young as eleven years old to be withdrawn from school for the sake of getting married. In health related matters, this practice is dangerous as sexual organ tissues of young girls are delicate and thus prone to rupture during sexual intercourse, which in turn creates entry points for HIV and other diseases (MCDGC, 2012).

   (d) Child Labour

   Although the government of the United Republic of Tanzania have made moderate advancement in efforts to eliminate child labour by launching National Costed Plan of Action for Most Vulnerable Children II (2013 - 17), the Human Rights Watch reports that children as young as eight years old are still working in small-scale gold mines in some regions of the country (HRW, 2013), (MoHSW, 2013a). In addition to mining, other forms of child labour involves dangerous activities in agriculture and fishing. Majority of these activities usually expose children to diseases.

   (e) Street Children

   Tanzania, as a country, also suffers from high number of street children in its developed regions, including Dar es Salaam, Mwanza and Arusha. Street children are highly vulnerable to illnesses such as fever, skin diseases, respiratory infections as well as injuries. In addition to these common diseases, majority of street children also engage in high-risk behaviours like unsafe sex and use of narcotic drugs, which increase their risk of contacting sexually transmitted diseases.

2. **Surface and Marine Regulatory Authority (SUMATRA)**

   (a) Marine Accidents

As a result of poor marine regulations, Tanzania suffers from severe marine accidents. It has been reported by SUMATRA that, between July 2012 and June 2013, 19 marine accidents involving 625 people were recorded in Tanzania (Mhagama, 2013). Out of 625 people involved, 380 were rescued and needed treatment from health care facilities across the country and the remaining died. These accidents reduces the number of available healthcare professionals further.

3. **Ministry of Energy and Minerals**
   (a) Invasion of the Mines

   The discovery of minerals in various parts of the country have also affected country's health-care system. With controlled mining activities, companies are provided with a deed from the government that allows them to legally mine in respective areas. Since majority of the citizens who live in close proximity to the mining areas are poor, it is common for them to invade and rob the mining areas while armed with knives and (sometimes) guns. In addition, it is a constant battle for the owners of the mining sites to stop illegal miners who usually attempt to steal mining resources, including rocks. Similar to other situations discussed so far, these battle between mining sites and citizens result into injuries and even deaths.

   (b) Mining Accidents and Health Risks

   The Ministry of Energy and Minerals in Tanzania has reported several cases of miners being covered by rubble while searching for pebble and other valuable minerals. The collapse of mine shafts, poor ventilation and lighting, poor mining methods and exposure to mercury and other hazardous substances are among the reasons for mining accidents and health risks in Tanzania. When these cases occur, healthcare facilities around the area and other specialised hospitals have to provide care services to the victims.

4. **Ministry of Health and Social Welfare (MoHSW)**
   (a) Malnutrition

   Due to social circumstances, children in Tanzania suffer from both under and over nutrition (Tanzania Food and Nutrition Centre, 2013). While over nutrition is experienced by well-off families, under nutrition is a challenge for poor families. In any case where a child suffers from mostly under nutrition, a social worker might be involved.

   (b) Low birth weight

   The higher degree of poverty results into low birth weight to many newborn babies in Tanzania. Among other reasons for low birth weight include illiteracy for expecting mothers, lack of antenatal care, pregnancy of adolescent girls (who may deliver low birth weight babies) and also pre-term delivery. Tanzania is positioned at number fifty five (55) in the world rankings.

   (c) Obstetric Fistula

   It is a condition where a hole is formed between vagina and bladder or vagina and rectum of a girl or woman during difficult child birth (MoHSW, 2001). This condition is common among girls and women who give birth at home because they are too poor to attend health clinics. On average, there are 3,000 new cases of obstetric fistula in Tanzania every year (CCBRT, 2011).

(d) Eclampsia

Eclampsia is one of the common problems facing majority of pregnant women in Tanzania (MoHSW, 2012). Majority of the women suffering from either pre-eclampsia or severe eclampsia have been caught up in several life endangering situations, including: falling down while walking, falling while they are alone at home or even falling while getting out of a car. When taken to a health care facility, and in particular public healthcare facilities, these patients are expected to receive all the treatment as required and payment should be issued later.

(e) Diabetes

Diabetes is now ranked as one of the major health challenges in the country, with an estimate of 1,706,930 cases (as of 2013). For any diabetic patient, they can choose to either attend public or private clinic. Although in both cases, patients are expected to pay after treatment, the cost is higher in private clinic compared to its public counterpart.

(f) Human Rabies

Tanzania healthcare system also suffers from cases of human rabies. Even though majority of these cases go unreported, on its February 2014 report, the MoHSW reported 512 cases of human rabies in the country compiled from twenty four regions (MoHSW, 2014).

Other context are as follows:

(a) Injuries at Work

The health care facilities in Tanzania also treat patients who were injured from their day to day jobs. In these situations, a patient will usually receive all the treatments required and then a healthcare facility will seek payment either from the patient, his employer or health insurance company, such as National Health Insurance Fund (NHIF).

(b) Surfing Injuries

As discussed in Chapter 2, Tanzania mainland is bordered by the long coast of an Indian ocean to the east. The healthcare facilities in Tanzania also attend individuals who may seek treatment due to injuries inflicted during surfing. Since healthcare facilities' main focus is saving lives, any patient with surfing injuries will receive treatment as any other case discussed earlier and a healthcare facility will seek payment later.

(c) Collapse of the Buildings

In Tanzania, there have been an increase in the number of building that are collapsing as a result of bad designing, faulty construction, foundation failure or even extraordinary loads. In addition to destroying the reputation of the construction industry, the collapse of the buildings also result into body injuries and even deaths. Those injured seek treatment from various healthcare facilities.

Papers used in Taxonomy

The following are the research works that has been used in Figure 3.16:

1. Downs, D.D., Rub, J.R., Kung, K.C. & Jordan, C.S. (1985). Issues in discretionary access control. In *2012 IEEE Symposium on Security and Privacy*, 208–208, IEEE Computer Society
2. Osborn, S., Sandhu, R. & Munawer, Q. (2000). Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies. *ACM Transactions on Information and System Security (TISSEC)*, **3 (2)**, 85 – 106
3. Sandhu, R., Coyne, E., Feinstein, H. & Youman, C. (1996). Role-Based Access Control Models. *Computer*, **29 (2)**, 38–47
4. Ray, I. & Kumar, M. (2006). Towards a Location-Based Mandatory Access Control Model. *Computers & Security*, **25 (1)**, 36–44
5. Sandhu, R. (1993). Lattice-Based Access Control Models. *Computer*, **26 (11)**, 9 –19
6. LI, L., HE, Y.Z. & FENG, D.G. (2004). A Fine-Grained Mandatory Access Control Model for XML Documents. *Journal of software*, **15**, 1528–1537
7. Ray, I., Kumar, M. & Yu, L. (2006). LRBAC: A Location-Aware Role-Based Access Control Model. *Information Systems Security*, 147–161
8. Sampemane, G., Naldurg, P. & Campbell, R.H. (2002). Access Control for Active Spaces. In *Proceedings 18th Annual Computer Security Applications Conference*, 343–352, IEEE
9. Covington, M.J., Moyer, M.J. & Ahamad, M. (2000). Generalized Role-Based Access Control for Securing Future Applications. Tech. rep., Georgia Institute of Technology
10. Bertino, E., Bonatti, P. & Ferrari, E. (2001). TRBAC: A Temporal Role-Based Access Control Model. *ACM Transactions on Information and System Security (TISSEC)*, **4 (3)**, 191–233
11. Joshi, J., Bertino, E., Latif, U. & Ghafoor, A. (2005). A Generalized Temporal Role-Based Access Control Model. *IEEE Transactions on Knowledge and Data Engineering*, **17 (1)**, 4 – 23
12. Hansen, F. & Oleshchuk, V. (2003). Spatial Role-Based Access Control Model for Wireless Networks. In *VTC 2003-Fall IEEE 58th Vehicular Technology Conference*, vol. 3, 2093–2097, IEEE
13. Bertino, E., Catania, B., Damiani, M. & Perlasca, P. (2005). GEO-RBAC: a Spatially Aware RBAC. In *Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies*, 29–37, ACM
14. Chandran, S.M. & Joshi, J.B. (2005). LoT-RBAC: A Location and Time-based RBAC Model. In *Web Information Systems Engineering – WISE 2005,*, 361–375, Springer
15. Kumar, M. & Newman, R.E. (2006). STRBAC-An Approach Towards Spatio-Temporal Role-Based Access Control. In *Communication, Network, and Information Security*, 150–155
16. Ni, Q., Trombetta, A., Bertino, E. & Lobo, J. (2007). Privacy-aware role based access control. In *Proceedings of the 12th ACM symposium on Access control models and technologies*, SACMAT '07, 41–50, ACM, New York, NY, USA

17. Bhatti, R., Bertino, E. & Ghafoor, A. (2005). A Trust-Based Context-Aware Access Control Model for Web-Services. *Distributed and Parallel Databases*, **18**, 83–105

18. Chakraborty, S. & Ray, I. (2006). TrustBAC: Integrating Trust Relationships into the RBAC model for Access Control in Open Systems. In *Proceedings of the eleventh ACM symposium on Access control models and technologies*, 49–58, ACM

19. Thomas, R. (1997). Team-Based Access Control (TMAC): a Primitive for Applying Role-Based Access Controls in Collaborative Environments. In *Proceedings of the second ACM workshop on Role-based access control*, 13–19, ACM

20. Thomas, R. & Sandhu, R. (1998). Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management. *Database Security*, **11**, 166–181

21. Oh, S. & Park, S. (2003). Task-Role-Based Access Control Model. *Information Systems*, **28**, 533–562

22. Karp, A., Haury, H. & Davis, M. (2009). From ABAC to ZBAC: The Evolution of Access Control Models. *Hewlett-Packard Development Company, LP*, **21**

23. Yuan, E. & Tong, J. (2005). Attributed Based Access Control (ABAC) for Web Services. In *Proceedings IEEE International Conference on Web Services ICWS 2005*, Ieee

24. Jin, X., Krishnan, R. & Sandhu, R. (2012). A Unified Attribute-Based Access Control Model covering DAC, MAC and RBAC. In *Data and applications security and privacy XXVI*, 41–55, Springer

25. Shen, H. & Hong, F. (2006). An Attribute-Based Access Control Model for Web Services. In *Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT'06. Seventh International Conference on*, 74–79, IEEE

26. Omary, Z., (2014) PhD Thesis

Related Publications

Analysis of the Challenges Affecting E-healthcare Adoption in Developing Countries: A Case of Tanzania

Zanifa Omary, Dennis Lupiana, Fredrick Mtenzi, Bing Wu
School of Computing
Dublin Institute of Technology
{zanifa.omary, dennis.lupiana}@student.dit.ie
{fredrick.mtenzi, bing.wu}@dit.ie

ABSTRACT: *Information and Communication Technologies (ICTs) have made significant impact on healthcare industry in the globe. Its adoption and use, which result into e-healthcare, has transformed the way healthcare services are delivered. Influenced by this transformation; medical errors and cost of delivering care have been reduced, while physician's efficiency and physician-patient relationship have been improved. The identified benefits and many others have influenced several governments in developed countries to reserve huge amount of money for stimulating its adoption. Unfortunately, there are many challenges affecting e-healthcare adoption in developing countries. In this paper we investigate and analyse challenges that hinder electronic healthcare adoption in developing countries and Tanzania in particular, and propose cost-effective solutions to them. The proposed solutions will help the Tanzanian government in its design and implementation of electronic healthcare projects.*

Keywords: E-healthcare, Developing countries, Challenges, Adoption, ICT

Received: 23 June 2009. Revised 19 July 2009, Accepted 28 July 2009

1. Introduction

Healthcare, either in paper-based or digital format, is an information-intensive industry as for the industry to operate; it depends on the existence of patient health information (PHI) that is collected whenever a patient visits a healthcare centre. The collection of PHI for paper-based or traditional healthcare setup is different from the collection when records are in digital form. The latter is also referred to as e-healthcare. Contrary to paper-based healthcare setup where PHI is collected every time a patient visits a healthcare centre, in e-healthcare physicians collect Personal Identifiable Information (PII) only once and frequently update its related medical records. In general term, e-healthcare is related to computerisation of electronic healthcare services.

Many developed countries such as Singapore, Canada, United States of America and United Kingdom have invested huge amount of money for stimulating e-healthcare adoption while developing countries are still dependent over the traditional healthcare setup. This huge investment by developed countries is motivated by the problems associated with the traditional healthcare setup such as duplication in patient's records, time wastage while preparing new records and increase in cost of delivering care due to duplication of tests and procedures. Such problems associated with the traditional healthcare setup can result in a PHI which is inaccurate, incomplete, outdated and irrelevant to physicians priority tasks and thus not helpful in healthcare management decision making (Igira *et al.*, 2007).

Although many countries, both developed and developing, understand the potential benefits of embracing e-healthcare, there are many challenges to be addressed prior to its adoption. These challenges which differ between countries include lack of patient unique identifier, lack of funds, low rate of Internet penetration and low bandwidth, lack of healthcare policies, lack of acceptable global standards and privacy, confidentiality and security concerns. In this paper we investigate and analyse challenges affecting e-healthcare adoption in developing countries and Tanzania in particular, and propose cost-effective solutions to them. The proposed solutions will help the Tanzanian government in its design and implementation of e-healthcare projects.

The rest of this paper is organised as follows: in section 2 the background of electronic healthcare, that is a review of its definitions and services offered, is provided. In section 3, benefits related to e-healthcare adoption are presented followed by the challenges facing e-healthcare adoption in Tanzania in section 4. Section 5 presents the proposed solutions to the challenges highlighted in section 4. Discussion is provided in section 6 followed by the conclusion and future work in section 7.

2. E-healthcare: Definition

The term e-healthcare or e-health came into use in the year 2000 and ever since has been broadly and vaguely defined (Pagliari *et al.*, 2005). The term has also been used as a synonym for health informatics, telemedicine, consumer health informatics and e-business. According to the research done by Pagliari et.al's (2005), e-healthcare definition varies with respect to its specified functions, stakeholder focus and specified technologies. In this section, we review and evaluate selected definitions based on the three categories and propose an appropriate definition that will be adopted for the rest of this paper.

Definition	**Strength/ Weakness**
"Healthcare delivery is being transformed by advances in e-health and computer-literate public. Ready to become partners in their own health and to take advantage of online processes, health portals and physician web pages and e-mail, this new breed of consumer is slowly redefining physician/patient relationship. Such changes can effect positive results like improved clinical decision making, increased efficiency and strengthened communication between physicians and patients" (Ball & Lillis, 2001)	This definition clearly identifies the source of transformation to e-healthcare and provides function that is offered through its adoption. However, based on the identified function we argue on the negative effects of exposing medical information with complex terminologies and descriptions to people with little or no medical training through the use of health portals. Its exposition may result into an increase in patient's anxiety and self harm from self diagnosis and treatment. Due to this biasness, this definition is considered inappropriate
"the use of the Internet for health purposes" (Provost et al., 2003)	This definition identifies Internet as the only technology to be used in e-healthcare. From research literature, there are different technologies related to the Internet that may be used, hence this definition is considered inappropriate
"E-health includes use of the internet or other electronic media to disseminate health related information or service" (Gustafson & Whyatt, 2004 May 15).	This definition is specific on a single function offered by e-healthcare that is dissemination of information. Other functions include storage and exchange of clinical data, computer based support, patient-provider interaction and many others (Pagliari et al., 2005).
"the use of emerging information and communication technologies, especially the Internet, to improve or enable health and health care" (Eng, 2001).	This is one among the general definitions that has been adapted by many researchers from the early emergence of the field. It provides the general functions that can be offered and technologies that may be used.
"An emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology" (Eysenbach, 2001 June 18).	It is also a general definition that has been adapted by many researchers such as Pagliari et.al's (2005). It indicates the originality of e-healthcare, functions offered together with technologies that may be used. As this definition is broadly defined, it is considered appropriate for this paper
"E-healthcare is an emerging field of medical informatics, referring to the organisation and delivery of health services and information using the Internet and related technologies. In broader sense, the term characterizes not only a technical development, but also a new way of working, an attitude, and a commitment for a networked, global thinking to improve health care locally, regionally, and worldwide by using information and communication technology" (Pagliari et al., 2005).	This definition has been adapted from Eysenbach (2001 June 18). From the original definition, authors have removed public health and business as the other two areas forming e-health. This indicates authors favour medical informatics and it is considered inappropriate.

Table 1. Selected Definitions of E-healthcare

From the evaluation of the selected definitions, as indicated in table 1, in this paper we adapt a generic definition from Eysenbach (2001 June 18) which was then adapted by many researchers (Pagliari et al., 2005).

Currently, the term e-healthcare, which is also referred to as the 21st century healthcare, has been identified to offer various services such as hospital information systems (HIS), Electronic Health Records (EHR) and telemedicine (Ouma & Herselman, 2008). However, EHR has been identified as the core application; as it provides electronic patients records which are input to other e-healthcare services (Grimson *et al.*, June 2000). Therefore in this paper our main focus will be on EHR and only a brief discussion will be provided on other e- healthcare services.

2.1 Hospital Information Systems (HIS)

Information systems (ISs) are usually designed to serve specific purpose in a specific industry or organisation where they are designated (Reichertz, 2006). From ISs definition and depiction in figure 1, HIS can be defined as an information sys-

Figure 1. Hospital Information System by Authors

tem designed to manage tasks in a hospital. According to Weber-Jahnke (2008), HIS is a comprehensive and integrated information system designed to manage administrative, financial and clinical aspects of a hospital. HISs can be composed of one or more software components with specialty-specific extensions as well as various subsystems in medical fields such as laboratory information systems.

2.2 Telemedicine

Telemedicine means the use of ICT for medical diagnosis and patient care when the healthcare provider and patient are geographically separated (Perednia & Allen, 1995). In e-healthcare settings, telemedicine can be as simple as two healthcare professionals discussing a case over the telephone or as complex as using satellite technology and video conferencing equipment to conduct a real-time consultation. Telemedicine has the potential to revolutionalise the way healthcare is delivered as it can reach into areas such as rural areas and in wars where traditional healthcare is difficult (Ouma & Herselman, 2008). Orlando (2007) argues that the adoption of telemedicine in developing countries is appropriate for addressing the problems that exist. These problems include high mortality and mordibility rates, high population and poor communication infrastructures. Despite its appropriateness, telemedicine is still not used in most developing countries due to insufficient requirements such as technologies that are required before its adoption

2.3 Electronic Health Records

Many researchers define and refer to EHR using different terms, such as computer-based patient records (CPR), computerised medical records (CMR), patient carried medical records (PMR) electronic patient records (EPR), electronic medical records (EMR), personal health records (PHR) and digital medical record (DMR). However, this paper adopts the definition provided by the Institute of Medicine, IOM, (2003) and Grimson (2001) which identifies EHR as the longitudinal collection of electronic patient records for and about patients where health information is pertaining to the health of an individual. Included in EHR is the information relating to a patient demographics, past medical history, progress reports, problems that the patient was or is facing, medication, laboratory data and radiology reports. These records have the ability to generate a complete record of a patient from cradle-to-grave (Grimson, 2001; IOM, 2003; Ouma & Herselman, 2008).

3. Benefits to e-healthcare adoption

The adoption and use of ICT has transformed several industries in the world (Wickramasinghe *et al.*, 2005). One among industries that has been transformed is healthcare, result into e-healthcare. There are various perceived benefits, to individuals and governments, associated with e-healthcare adoption. These benefits include reduction in medical errors, an improvement on physician efficiency, and improvement in physician-patient relationship and cost involved in delivering care. This section provides a discussion of these benefits followed by challenges to e-healthcare adoption in Tanzania in the next section.

3.1 Improvement in physician efficiency

In 2001, Eysenbach (2001 June 18) in his article "What is e-health?" highlights 10 promissory e's in e-health. Efficiency is one among those promises; other e's stand for enhancing quality of care, evidence-based, empowerment, encouragement, education, enabling, extending, ethics and equity. Theoretically, with the adoption of e-healthcare where patient's EHRs are readily available anytime in e-healthcare information systems, physicians will be able to attend more patients compared

to the physician working in a traditional healthcare setup. However, physicians do not generally agree on this benefit, they consider the whole process of obtaining patients records from a range of computer applications as not a clinical skill and wastage of time hence resisting their adoption.

3.2 Improvement in the quality of care

There are two ways that the adoption of e-healthcare can improve the quality of care to patients. The first way is through patients' and physicians' use of health web portals. With the presence of health web portals, patients can search for medical and related information hence improving their knowledge regarding healthy lifestyles, health and self-treatment. Additionally, physicians can search for health information on the web for education and research. An Irish citizen, for instance, can go online and find almost everything they need to know about health. The second way that e-healthcare adoption improves the quality of care of the patients is through collaboration between physician's located in different areas within the country while delivering care. This collaboration can be done through video conferencing where physicians in different areas can discuss issues pertaining to a patient. However, this knowledge sharing is difficult due to nature of their work, technological concerns and privacy, security and confidentiality concerns.

3.3 Improvement in Patient- Physician relationship

With its capacity to allow inexpensively retrieval of information anywhere, anytime, Internet is already creating strong physician-patient relationship. In fact even the word patient as used in traditional healthcare is now being replaced with *consumer* in e-healthcare. In developed countries for example, this strong relationship is influenced by the amount of sensitive patient information that is shared between these two groups; as physicians know all about health information of their patients from patient's body to the state of the health (Sharma *et al.*, 20 March 2005).

4. Cost saving

With e-healthcare, there is an existence of digital imaging services that can virtually eliminate the need for films and x-rays. Nowadays, radiology department for example, in healthcare centres which have adopted e-healthcare can send digital x-ray films to healthcare providers' notebooks and handheld devices as well as mounting devices hence reducing costs. Cost can also be reduced through cutting back unnecessary tests and treatments. In the United States of America for example, a Congressional Budget Office report indicates that health information technology (IT) provisions of the federal economic stimulus package could help the federal government reduce Medicaid and Medicare costs by more than $ 12 billion over the next 10 years which is nearly $ 1.2 billion a year. The saved money can be used in other sectors and hence contributing to the economy of the country.

Due the presence of these benefits, several countries around the globe especially developed countries are investing huge amount of money for e-healthcare adoption. Contrary to developed countries, developing countries are still dependent over the traditional healthcare setup. In the next section we investigate and analyse challenges that hinder e-healthcare adoption in developing countries and cases from Tanzania will be presented.

5. Challenges to e-healthcare adoption: case of Tanzania

While the integration of ICT and healthcare has brought a lot of potential benefits, there are many challenges which affect its adoption. In 2004, the World Health Organisation (WHO) (2004) presented challenges that developing countries face in adopting e-healthcare, and EHR in particular. Likewise, many researchers have also identified challenges associated with e-healthcare adoption in developing countries (Androuchko, 2004; Sharma *et al.*, 2006; Sood *et al.*, 2008; WHO, 2006b). However, these challenges are not tailored to a specific country. In this section challenges to e-healthcare adoption in developing countries with cases from Tanzania will be discussed. Solutions to these challenges will be provided in section 5. The section begins with an overview of the healthcare sector in Tanzania.

6. Tanzania Healthcare Sector

Tanzania is administratively divided into 2, Tanzania Mainland which consist of 21 regions and Tanzania Island also known as Zanzibar which consists of 2 regions. Among the 21 regions in Tanzania mainland consist of Dar es Salaam, Dodoma, Rukwa, Morogoro, Arusha, and many others. Tanzania Island consists of Unguja and Pemba. The regions are further divided into districts.

The population distribution in Tanzania is extremely uneven as more than 80 percent of the population live rural areas leaving 20 percent for urban and other residing in foreign countries. Tanzania has more than 130 ethnic groups but the national language is Swahili, which is a Bantu language, with strong Arabic and English borrowings. The other official language is English.

The health infrastructure and healthcare services are provided through three main levels, namely, primary care level comprising of the first and second line healthcare units and primary healthcare centres, secondary level which consist of district hospitals and tertiary level consisting of specialised hospitals such as Muhimbili and Mnazi Mmoja in Tanzania mainland and Tanzania island respectively (Igira et al., 2007). The healthcare setup is traditionally based and is faced with a number of problems from compiling, analysing, and reporting to the management of healthcare data. With these challenges, it is of importance to examine challenges that hinder e-healthcare adoption in developing countries and Tanzania in particular.

6.1. Lack of Patient's Unique Identifier

Johns (2002) defines Patient Unique Identifier (PUI) as a single unique number assigned to each patient within a hospital that distinguishes one patient and his or her records from all others. Therefore, since EHR contains sensitive patient records from cradle to grave, it is necessary to have PUI to differentiate patient's records. However, due to cost involved in its generation, only few countries are using PUIs. The majority opt for alternative solutions such as citizen unique identifiers.

Unfortunately, things are not the same in Tanzania. Although there have been efforts to establish National Identity Cards (NIC) since 1968, which can be used as a citizens' unique identifier, this has not yet occurred due to a number of reasons. It is only recently, in 2007, that the government of Tanzania has agreed on the establishment of a NIC scheme under the National Identification Authority (NIDA).

6.2. Lack of funds

The lack of funds is one of the major problems facing e-healthcare adoption in many developing countries. As a result of the lack of funds to control their own projects, many developing countries largely depend on foreign aids. For Tanzania, these foreign aids from developed countries are even controlling the whole economy of the country by looking on the percentage of budgets dependence. The Tanzania's budget in the year 2007 depended on foreign aid by 42 percent and the expectation was to reduce the dependence rate to 34 percent in 2008 (Mkulo, 2008). As a result of ongoing dependency on foreign aids that is, monetary and through resources, many e-healthcare projects which are funded by developed countries, is often directed to certain diseases such as HIV/AIDS. Therefore, e-healthcare adoption in developing countries is limited to certain diseases and is not available generally within the country.

6.3. Low rate of internet penetration and low bandwidth

According to the International Telecommunication Union, ITU, (2007), by the year 2006, the Internet penetration in Tanzania was 1 percent of the population compared to 6.0, 7.9 and 10.5 percent of the population in Nigeria, Kenya and South Africa respectively. The low rate of Internet penetration and low bandwidth are among the challenges to e-healthcare adoption in Tanzania. Due to the poor ICT infrastructure, the majority of areas in the country cannot support Internet deployment, which in turn, hampers e-healthcare adoption. In urban areas, where there is considerable Internet penetration, there is low bandwidth which again hampers its utilisation. The slow adoption to ICT in developing countries is influenced by several factors such as the perception of its leaders as it is a misallocation of resources, politics and ICT not being a priority of the country. Therefore, since EHRs need to be shared between physicians located in different healthcare centres, these factors subsequently hinder its adoption and use. Other factors apart from low rate of Internet penetration that hinder EHR sharing include technological concerns, privacy, and security and confidentiality concerns.

6.4. Lack of healthcare policies

Policy, as defined in Oxford English Dictionary (OED, 1989), is a purposeful plan of action to guide decisions and achieve rational outcomes. In the context of the healthcare industry, healthcare policies are responsible for providing evidence-based, peer reviewed policy guidance and resources to support advocacy decision making at the local level. Additionally, healthcare policy creates a framework to provide necessary conditions for the implementation of health promotion activities, and interventions by using particular tools such as laws, policy measures, policy documents and agreements. The lack of these

policies will pose another challenge in e-healthcare since those responsible for making decisions will make them without guidance. Most developed countries and some developing countries such as South Africa have healthcare policies in place to guide the deliverance of electronic healthcare services; however in Tanzania there is no healthcare policy related to the delivery of e-healthcare services.

6.5. Lack of acceptable standards

For future processing of EHRs, chosen computer systems should be able to identify data in one system and associate them with data located in other systems (Wickramasinghe et al., 2005). This is accomplished by the existence of standards for different uses. In developed countries such as United Kingdom and United States of America, there is a huge amount of research institutions trying to establish standards for different uses.

Among the established standards is Healthcare Level 7 (HL7) for transmission of e-healthcare information, SNOMED CT (Systematised Nomenclature for Medicine Clinical Terms) developed by the College of American Pathologists and National Health Service (NHS) in England (SNOMED-International, 2009) and CEN 13606 for the exchange of shared EHR. However, there are no acceptable standards agreed to be used globally in e-healthcare. Politics at an international level which involve companies and organisations that develop e-healthcare standards is one among the reasons for the lack of acceptable global standards. The lack of acceptable global standards is also influenced by historical reasons and digital divide.

6.6. Lack of manpower

Another challenge for e-healthcare adoption in developing countries is the availability of an adequately skilled healthcare workforce. In a study by Sood et al.'s (2004) which examined challenges that healthcare workforce face while implementing telemedicine technology in India, computer literacy was considered to be the main challenge. This may be the same in Tanzania. As shown in figure 2, there are few physicians, pharmacists, dentists and technicians while the major group comprises of nurses and midwives and other healthcare workers. The latter group is characterised by the low level of education compared to the previous group. With an unequal distribution between these two groups, e-healthcare adoption will succeed more slowly when compared to a situation when the distribution is more equal.

7. ICT challenges

The majority of developing countries population live in rural areas. According to the Tanzanian Government website, 80 percent of its total population live in rural areas (Government, 2009). The ICT, which is the backbone to e-healthcare adoption and implementation, is still out of reach for this large group due to a number of reasons:

Access cost: According to International Monetary Fund, IMF, (IMF, 2005) in 2004, roughly half of the world population live on less than one dollar a day. Most of these people reside in developing countries. Contrary, access to ICT in these developing countries involve large amount of money which many potential users can not afford.

Education: Despite opting for ICT in their day to day tasks, many organisations in developing countries lack security awareness programs for their employees. According to Desman (2001), security awareness refers to employees' understanding on security control measures and their consequences. The lack of security awareness programs increases the chances of security breaches. On a survey done by Lupiana (Lupiana, 2008), identified a huge gap on computer security perception between developed and developing countries where Tanzania was considered as a case for developing countries.

Language: Poor literacy is another major problem related to ICT, such as the Internet, in developing countries. As majority of the population in developing countries reside in rural areas, they are divided into regions which speak different native languages. And for those who can read, may know only a local language such as Swahili in Tanzania while Internet is dominated by English-language.

8. Privacy, confidentiality and security concerns

Despite the presence of other challenges that countries may face in its adoption to e-healthcare; privacy, confidentiality and security are the three important challenges involved in protecting patient healthcare information from accidental or intentional misuse (Maheu *et al.*, 2001). According to Rindfleish (August 1997), in e-healthcare context, privacy is defined as the right and desire of an individual to control the collection, use and disclosure of his or her health information while confidentiality

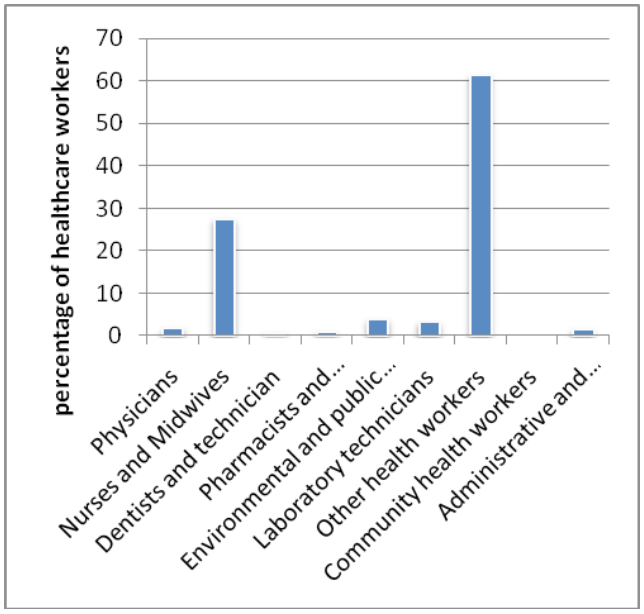


Figure 2. Healthcare workforce distribution in Tanzania (WHO, 2006a)

refers to the controlled release of personal health information to a care provider or information custodian under an agreement that limits the extent and conditions under which that information may be used or released further.

The confidentiality of the patient healthcare information may be broken either internally, by accidental disclosure, insider curiosity or by an insider subornation or may be broken from outside intrusion through unauthorised access (Kelly & Unsal, 2002). Security is defined as methods such as policies, procedures or safeguards by which access to patient health information is controlled and protected from accidental or intentional disclosure to unauthorised persons, and from alteration, destruction and loss (Maheu et al., 2001; Rindfleisch, August 1997).

IT solution companies are among the main enforcers to e-healthcare adoption and implementation. These companies are interested with the financial gain from e-healthcare products that they produce. They concentrate much in producing usable products and hence causing security to suffer. Insufficient security which causes breaches in e-healthcare information systems results into privacy, security and confidentiality concerns. These three are also the major challenges in developed countries. Other challenges in developed countries include

8.1 Resistance to Information and Communication Technology

IT solution companies claim over a number of benefits, such as reduction in medical errors and cost of delivering care and improvement in physician efficiency that can be offered through e-healthcare adoption. Despite being outlined with these benefits, healthcare professionals still resist to incorporate computer technology while attending patients. These professionals prefer to write prescriptions for example by hand rather than using the technology more efficiently. The resistance has been associated with a number of reasons. Healthcare professionals claim the whole process of obtaining patients records from a range of computer applications as not the clinical skill and wastage of time. For developing countries Sprague (September 29, 2004) and Sood et.al (2008) identify lack of training in ICT and computer illiteracy as the source of healthcare professionals resistance. For a successful implementation of e-healthcare in the world, computer skills to all healthcare professionals and staff involved in the process is a must.

8.2 Number of breaches in e-healthcare information systems

E-healthcare is an information-intensive industry as it contains sensitive information about an individual that may cause identity theft and social stigma to an individual if compromised. This information is also referred to as electronic health record (EHR). The electronic healthcare record is processed and stored in electronic healthcare information systems (Haux, 2006). Influenced by the type of information that is processed and stored in these systems, a number of breaches from within

or outside an organisation keep on increasing. When users learn about these breaches, get worried about their privacy and hence resist e-healthcare adoption. For the organisations where these breaches occur or their products are associated with the breaches may suffer from reputation of their brand and from legal liability.

8.3 Fear of losing control of their data

The shift from traditional healthcare to e-healthcare involves the transformation of records from paper-based to digital format. These records are referred to as Electronic Healthcare Record (EHR). Grimson (2001) defines and characterises the next generation EHR as the longitudinal cradle-to-grave records readily accessible and available over the Internet. These records will be linked to clinical protocols and guidelines to drive the delivery of healthcare to the individual. The presence of these records over the Internet facilitates record sharing between physicians. However, patients usually feel that they are losing control of their data hence resisting e-healthcare adoption.

8.4 Poor e-healthcare systems design

Many e-healthcare systems are developed by Information Technology (IT) solution companies which operate for the purpose of getting profit. These companies are interested with the financial gain from e-healthcare products that they produce. They concentrate much in producing usable products for healthcare institutions and hence causing privacy, security and confidentiality to suffer. In order to resolve this, efforts to secure e-healthcare systems need to be taken from design of the systems to implementation in order for the developments that have been achieved so far to be rolled to the real world.

8.5 Proposed Solutions

In this section we propose solutions to the challenges identified in section 4 as follows: Using birth certificates as an alternative PUI, cheaper operating systems for e-healthcare software, the improvement of computer infrastructures, and in-service training and incorporation of new syllabus as training procedures.

8.6 Alternative Patient Unique Identifiers

We are proposing the use of birth certificate numbers as an alternative solution to uniquely identify individuals when adopting e-healthcare and EHR in particular in Tanzania. Although national IDs, blood donor IDs and mother's maiden names have been proposed as alternative solutions in other developing countries (WHO, 2006b), these solutions are inappropriate. For instance, the use of national IDs as an alternative may result into several problems such as service overload as the same ID is used in more than one system. As previously described EHR have to exist from cradle to grave, however national IDs are given to those aged 18 years and above, this will result into e-healthcare delivery bias as only adults would benefit from the service.

Moreover, with blood donor IDs, only few citizens participate in blood donation. As a result only few possess these IDs. Therefore, both national and blood donor IDs are inappropriate alternatives as they are only limited to a small group of citizens. Additionally, mother's maiden name is also becomes an inappropriate alternative solution to PUI when a single mother has two or more children. This may result in easy compromises and hence threaten the privacy of individuals. Therefore, birth certificate number remains as an appropriate alternative for PUI in Tanzania.

The Tanzania Birth and Death Registration Act was first established on the 15th of December 1920 aiming to make provision for the registration of births and deaths and for the issue by medical practitioners of certificates of the cause of death (RITA, 2009). The Birth and Death Act allows every child born alive after the commencement of this Act to be registered within three months of birth by father, mother, occupier of the house in which to his knowledge such child is born, person present at the birth or the person having charge of such child. Upon registration, each child receives a uniquely enumerated birth certificate. As every individual is eligible to receive a birth certificate this is an appropriate PUI, as it can uniquely identify all citizens, young and old.

8.7 Free and Open Source Software (FOSS)

In relation to the lack of funding for e-healthcare adoption in Tanzania, we are proposing the deployment of FOSS in healthcare industry. There are huge amount of FOSS, ranging from operating systems such as Linux to e-healthcare software such as Care2X (Care2X, 2009) and openEHR (openEHR, 2009). Since the majority of developed countries such as the United Kingdom, Sweden and Singapore have engaged themselves in using FOSS such as Care2X and openEHR in e-healthcare implementation; it is therefore plausible for developing countries and Tanzania in particular to adopt FOSS. Additionally,

since proprietary software involves licensing which is often too expensive, by deploying FOSS we are definite that the cost of deploying and running e-healthcare will be reduced.

8.8 Proper cost evaluation

To resolve the issue of perception of cost and ROI, cost evaluators in Tanzania should learn from ongoing e-healthcare projects in other developing countries and take proper initiatives to evaluate e-healthcare projects on a long-term basis. They need to make proper comparisons between the cost of current systems and the perceived cost of the intended new e-healthcare systems against the proposed benefits that the country might receive (WHO, 2004). This evaluation will help the government and individuals to understand the benefits of these projects and hence resolve the misleading notion of e-healthcare projects involving high costs.

8.9 Computing infrastructure Improvement

Computer infrastructure is the backbone to e-healthcare services implementation. However, Tanzania, for the proper adoption of e-healthcare, must first deploy computers and computer systems for use in the healthcare industry before adopting e-healthcare fully. E-healthcare can then provide more services which requires more technology integration such as telemedicine (Perednia & Allen, 1995). Additionally, the government has to control computer and computer systems prices, so that the majority of people can possess them, as well as controlling Internet access costs.

8.10 Training

As highlighted in figure 2, most of healthcare workers in Tanzania are Nurses and Midwives and other healthcare workers. These groups form 80 percent of overall healthcare workers. Unfortunately, these workers lack computer skills as well as general skills for the use of E-healthcare information systems. For the proper implementation of e-healthcare in Tanzania, this group should be offered in-service training as they can eliminate manpower issues in short term basis. As a short-term solution, in service training is the appropriate way to ensure availability of the required skills at the required time. To support this, WHO (2006b) highlighted the need for a basic form of training if e-healthcare has to be implemented in a country.

In the long-term, healthcare institutions, where Nurses and Midwives and other healthcare workers are trained, should incorporate e-healthcare syllabus to its respective courses.

8.11 Regulations

In relation to the privacy, confidentiality and security concerns in e-healthcare adoption, strong security and regulation measures need to be taken into consideration by the Tanzanian government. For the case of security concerns such as unauthorised access to e-healthcare information systems which might cause social embarrassment, prejudice or affect insurability, technological security tools such as encryption and access control are in place to help protect sensitive patient healthcare information. Although we propose security tools to address security concerns, regulations are appropriate for protecting the privacy of individuals. The Tanzanian government have to establish regulations for protecting privacy of its citizens before e-healthcare adoption. One among the regulations established for protecting privacy of individuals is HIPAA, *Health Insurance and Portability and Accountability Act*, (1996) from the United States of America.

8.12 Discussion

One major obstacle in e-healthcare adoption, either in developed or developing countries is privacy, confidentiality and security of e-healthcare information systems. The American government, for instance, for the year 2009 reserved $ 19 billion for stimulating e-healthcare adoption. However, despite this huge investment, e-healthcare adoption in the USA is still stumbling. Its users such as physicians are not sure about the security of e-healthcare information systems and hence resisting their deployment and use. Additionally, patients are also concerned about the privacy of their medical records. This has been influenced by a number of existing cases involving breaches in e-healthcare information systems. However, we argue that e-healthcare adoption is not a monetary problem per se. It goes beyond, to involve human trust. Therefore, despite focusing on securing funds for e-healthcare deployment, developing countries have to consider the human element as well.

The lack of PUIs is another big challenge for e-healthcare adoption in developed and developing countries. Although some developed countries have specific PUIs, majority are still opting for existing alternative solutions. For instance, the Republic of Ireland has proposed the use of Social Security Number (SSN) as an alternative to PUIs while we propose to use birth

certificate numbers as an alternative for PUI in Tanzania. In this paper we propose the use of birth certificate numbers, which every citizen in Tanzania is legally entitled to possess, for the sake of saving cost as opposed to the national IDs which are costly to generate and can result in service overload and will create bias to those who can and cannot receive e-healthcare services due to age. To possess a birth certificate in Tanzania costs less than two dollars. However, the use of birth certificates may also result into service overload. This is not much of a concern as we lack funding to support these projects; we need to seek cost-effective solutions that are beneficial to developing countries. The only big challenge that will be faced by the use of birth certificates is that not all citizens are aware that they are legally allowed to possess birth certificates. This can be overcome by the provision of education to individuals, especially in rural areas.

Although we propose the use of Free and Open Source Software (FOSS) (from operating system to EHR software) due to the lack of funds, these products are associated with a number of challenges. As these products are *"free"*, its users lack support and maintenance from development teams. The Tanzanian government needs to reserve enough funds for staff training in the healthcare industry. If e-health is to flourish in Tanzania, it needs to be staged and nurtured. We need to build on our own local skills and infrastructure, based on local demand. Table 1 provides a summary of issues, challenges and their suggested solutions.

Issues and Challenges	**Proposed Solution**
Lack of patient's unique identifiers	Using Birth Certificates Numbers which are uniquely enumerated
Lack of funds	Using FOSS such as Linux and open EHR to reduce cost
Lack of standards	Using e-healthcare standards adopted by other developing countries such as HL7
Manpower issues	Short term and long term training strategies
ICT challenges	Adopt systems that can work in hostile environments, government control over access cost, customisation of the systems into local languages

Table 2. Issues, Challenges and its Suggested solution

8.13 Conclusions and Future Work

From research literature, developed and developing countries face different challenges while adopting e-healthcare. Despite offering several benefits, lack of patient unique identifier, lack of funds, low rate of Internet penetration and low bandwidth, lack of healthcare policies and lack of acceptable global standards are among the common challenges hindering e-healthcare adoption in developing countries. In this paper we have identified challenges that developing countries particularly Tanzania will face while adopting e-healthcare. Based on these challenges we have also proposed cost-effective solutions that will help the government of Tanzania in its design and implementation of electronic healthcare projects.

Additionally, apart from the identified challenges; privacy, security and confidentiality are among the common challenges to both developed and developing countries. As a future work we propose research to be carried out to identify appropriate security to be implemented in FOSS e-healthcare information systems. As the users of e-healthcare information systems such as physicians, patients and insurance companies resist their use due to security concerns, assuring their security will boost their trust and hence boost their adoption.

References

[1] Androuchko, L. N. I. (2004). Developing countries and e-health services. *In*: Paper presented at the 6th International Workshop on Enterprise Networking and Computing in Healthcare Industry.

[2] Ball, M. J., Lillis, J. (2001). E-health: Transforming the physician/patient relationship. *International Journal of Medical Informatics* - 61, Issue 1, p. 1-10.

[3] Care2X. (2009). Care2x: Integrated healthcare environment. From http://www.care2x.org/
[4] Desman, M. (2001). Building an information security awareness program: AUERBACH.
[5] Eng, T. R. (2001). The ehealth landscape: A terrain map of emerging information and communication technologies in health and health care: The Robert Wood Johnson Foundation.
[6] Eysenbach, G. (2001 June 18). What is e-health? Journal of Medical Internet Research, 3 (2).
[7] Government, T. (2009). Water: The 21st annual water experts conference (awec). Retrieved March 5, from http://tanzania.go.tz
[8] Grimson, J. (2001). Delivering the electronic healthcare record for the 21st century. International Journal of Medical Informatics, 64, 111-127.
[9] Grimson, J., Grimson, W., Hasselbring, W. (June 2000). The SI challenges in health care. Communication of the ACM, 43 (6) 49-55.
[10] Gustafson, D. H., Whyatt, J. C. (2004 May 15). Evaluation of ehealth systems and services. BMJ.
[11] Haux, R. (2006). Health information systems-past, present, future. International Journal of Medical Informatics, 75, 268—281.
[12] HIPAA. (1996). Understanding hipaa privacy.
[13] Igira, F. T., Titlestad, O. H., Lungo, J. H., Makungu, A., Khamis, M. M. (2007). Designing and implementing hospital management information systems in developing countries: Case studies from Tanzania – Zanzibar. Health Informatics in Africa (HELINA).
[14] IMF. (2005). India: 2004 article IV consultation—staff report; staff statement; and public information notice on the executive board discussion. Retrieved March, 2009, from http://www.imf.org/external/pubs/ft/scr/2005/cr0586.pdf
[15] IOM. (2003). The computer-based patient record: An essential technology for health care, revised edition: Institute of Medicine.
[16] ITU. (2007). Telecommunications/ict markets and trends in Africa.
[17] Johns, M. L. (2002). Health information management technology: An applied approach. American Health Information Management Association.
[18] Kelly, E. P., Unsal, F. (2002). Health information privacy and e-healthcare. *International Journal of Healthcare Technology and Management*, Issue: 4, (1-2) 41-52.
[19] Lupiana, D. (2008). Development of a framework to leverage knowledge management systems to improve security awareness. Dublin Institute of Technology, Dublin.
[20] Maheu, M., Whitten, P., Allen, A. (2001). *E-health, telehealth, and telemedicine: A guide to start-up and success* . San Francisco: Jossey-Bass.
[21] Mkulo, M. (2008). The estimates of government revenue and expenditure for the financial year 2008/09: Parliament of Tanzania.
[22] OED. (1989). *Oxford English dictionary*: Oxford English Press.
[23] openEHR. (2009). OpenEHR: Future-proof and flexible. from http://www.openehr.org
[24] Orlando, M. (2007). Is your healthcare it solution the answer to the needs of the developing world? *Healthcare Computing*, 144-152.
[25] Ouma, S., Herselman, M. (2008). *E-health in rural areas: Case of developing countries.* Paper presented at the Proceedings of the World Academy of Science, Engineering and Technology.
[26] Pagliari, C., Sloan, D., Gregor, P., Sullivan, F., Detmeter, D., Kahan, J., et al. (2005). What is ehealth (4): A scoping exercise to map the field. *Journal of Medical Internet Research,* 7 (1).
[27] Perednia, D. A., Allen, A. (1995). Telemedicine technology and clinical applications. *JAMA*, 483-488.
[28] Provost, M., Perri, M., Baujard, V., Boyer, C. (2003). Opinions and e-health behaviours of patients and health professionals in the U.S.A and Europe. *Stud Health Technol Inform, 95*, 695-700.
[29] Reichertz, P. L. (2006). Hospital information systems——past, present, future. *International Journal of Medical Informatics - Elsevier,* 75, 282—299.
[30] Rindfleisch, T. C. (August 1997). Privacy, information technology and health care. *Communications of the ACM,* V. 40 (8) 92-100.
[31] RITA. (2009). The birth and death registration act: RITA.
[32] Sharma, S. K., Ahmed, N., Rathinasamy, R. S. (20 March 2005). E-healthcare: A model on the offshore healthcare delivery for cost saving. *International Journal of Healthcare Technology and Management,* V. 6 (3) p. 331-351 (321).
[33] Sharma, S. K., Xu, H., Wickramasinghe, N., Ahmed, N. (2006). Electronic healthcare: Issues and challenges. *International Journal of Electronic Healthcare,* 2 (1) 50 - 65.
[34] SNOMED-International. (2009). Snomed clinical terms fundamentals as of February 2009. *Available at http://www.ihtsdo.org*.

[35] Sood, S. P. (2004). Implementing telemedicine technology: Lessons from India. *World Hospital and Health Services (International Hospital Federation),* 40 (3) 29-31.
[36] Sood, S. P., Nwabueze, S. N., Mbarika, V. W. A., Prakash, N., Chatterjee, S., Ray, P., et al. (2008). Electronic medical record: A review comparing the challenges in developed and developing countries. *In:* Proceedings of the 41st Hawaii International Conference on System Sciences, 1-10.
[37] Sprague, L. (September 29, 2004). Electronic health records: How close? How far to go? *National Health Policy Forum Issue Brief,* (800) 1-17.
[38] Weber-Jahnke, J. H. (2008). *Encyclopaedia of healthcare information systems*: Idea Group Inc.
[39] WHO. (2004). *Developing health management information systems: A practical guide for developing countries*. Geneva: World Health Organisation.
[40] WHO. (2006a). *Africa health workforce observatory: Hrh fact sheet Tanzania*.
[41] WHO. (2006b). Electronic health records: Manual for developing countries. *World Health Organisation*.
[42] Wickramasinghe, N., Fadalla, A. M. A., Geisler, E., Schaffer, J. L. (2005). A framework for assessing e-health preparedness. *International Journal of Electronic Healthcare*, 1 (3) 316-334.

Authors Biography

Zanifa Omary is an Assistant Lecturer at the Institute of Finance Management (IFM), Dar es Salaam, Tanzania. She received her MSc. degree in Computing (Information Technology) at the Dublin Institute of Technology, Ireland and Advanced Diploma in Computer Science at the Institute of Finance Management, Tanzania. She is currently pursuing her PhD studies in e-healthcare information systems security. Her research interests include Information systems security, Machine Learning, Data Mining and Serious Games.

Dennis Lupiana is an Assistant Lecturer at the Institute of Finance Management (IFM), Dar es Salaam, Tanzania. He is a Masters Degree holder in Computing (Knowledge Management) from the Dublin Institute of Technology, Ireland. He pursued his undergraduate studies at the Institute of Finance Management majoring Information Technology, and Dar es Salaam Institute of Technology (DIT) majoring Telecommunications Engineering. Currently he is pursuing PhD studies in developing a multi-domain knowledge sharing framework to support user mobility in ubiquitous computing environments. His research interests include Knowledge Management, Web Ontology Languages, Wireless Sensor Networks, Session Mobility, and Computer Security.

Dr. Fredrick Mtenzi is a Lecturer at the School of Computing, Dublin Institute of Technology (DIT), Ireland. Prior to joining DIT, he worked as a Lecturer and Consultant at the University of Dar es salaam in Tanzania. He did his undergraduate studies at the University of Dar es salaam in Tanzania and his MSc. and PhD from the University College Dublin in Ireland. His research interests includes design and implementation of algorithms for solving combinatorial optimisation problems, energy aware routing in mobile ad hoc networks and its related security issues, cybercrime, Ubiquitous computing and knowledge management.

Dr. Bing Wu received his B.Sc. and M.Sc. in Computer Science from the National University of Defense Technology, China in 1982 and 1985, respectively. He received a Ph.D. in the Computation Department of the University of Manchester, Institute of Science and Technology (UMIST), UK in 1996. After the Ph.D. study, he worked as a Research Fellow in the Department of Computer Science, Trinity College Dublin from 1996 to 1998. On November 1998, he joined the Computer Science Department of the Dublin Institute of Technology (DIT). He is currently the Head of the Computer Science Department within the School of Computing.

Context for Securing EHRs in a Dynamic Healthcare Environment

Zanifa Omary[1], Fredrick Mtenzi[2], Bing Wu[3]

School of Computing,
Dublin Institute of Technology,
Kevin Street, Dublin 8, Dublin, Ireland
[1]Zanifa.Omary@dit.ie
[2]Fredrick.Mtenzi@dit.ie
[3]Bing.Wu@dit.ie

***Abstract*— Although many of the healthcare decisions are influenced by individual's characteristics and choices, highly dynamic nature of the healthcare environment has introduced numerous challenges to EHRs such as privacy and security. Some accumulating evidences show that adding context in an access control model can help improve the security of EHRs by providing dynamic levels of access to the records while taking into consideration environmental and healthcare professional's context. Contrary to its promises, when appropriately used, researchers in the healthcare environment are still using contextual attributes proposed by researchers from other domains such as Ubiquitous Computing (UbiComp). This act, in turn, reduces the rate of protection of EHRs as different domains consider some contextual attributes to be more important than the other.**

Again, with the nature of information that is collected, processed and stored using Electronic Healthcare Information Systems, close attention should be paid out to who controls what is gathered, who has access to it and where that information is stored. Taking into consideration the need of knowing where EHRs are stored, then contrary to identity, location, time and activity, which are mostly used in UbiComp and other domains, in our ongoing work, we propose to use subject, time and activity while replacing location with resource as location cannot stand on its own without resource or subject to be associated with it.

In this paper we investigate how rich in context the general healthcare environment is and thereafter propose relevant contextual attributes for the domain. The proposed contextual attributes will be used as a guideline while identifying specific contextual attributes for the Tanzania's healthcare environment as different healthcare workflows have different context that need to be considered important. The approach being adopted for our main research is by adding specific contextual attributes, from the Tanzania's healthcare environment, into the Role Based Access Control model while developing a dynamic context-aware access control model for securing EHRs in Tanzania.

***Keywords*— Electronic Healthcare Record, Context, Access Control, Dynamic Healthcare Environment**

I. INTRODUCTION

The concept of context intersects with a diverse range of research from Artificial Intelligence (AI), Ontology, Knowledge Representation to healthcare [1]. With this multiplicity of domains where context has been differently defined and various contextual attributes have been proposed, it is therefore, not obvious to define context. However, in order to propose contextual features also known as contextual attributes that need to be considered while providing healthcare professionals with dynamic levels of access to patient's Electronic Healthcare Records (EHRs), clear definition of context as well as relevant contextual attributes from the domain need to be provided [2]. The term dynamic levels of access to patient's records means healthcare professionals will be provided with varying levels of access to the records depending on contextual attributes gathered. Consider, for example, two healthcare professionals requesting access the John's EHRs; the first healthcare professional is requesting to access records while outside of the healthcare centre and the other is in the ward (within the hospital). While considering location (context) before providing access, then these two professionals will be provided with two different levels of access to the record as the latter may be provided access to only basic information while the other being given full access.

For the whole hospital, context tends to improve operational efficiency by integrating real time contextual information, such as location and status of medical equipment and staff, into the healthcare workflow. As a result, context enhances the quality of patient care, increases staff efficiency while helping the healthcare organisation manage capital and operational costs. In relation to patients in general, context enables access to environmental information, such as temperature or humidity, to provide an optimal patient experience [3] while to patient's records, the inclusion of contextual attributes may result into healthcare professionals to be provided with dynamic levels of access to the records and hence ensuring confidentiality as well as security of records .

As an example, consider the following scenario for the applicability of the contextual attributes in the dynamic healthcare environment.

Within a hospital, a healthcare professional can move between theatre, ward, pharmacy, office, front desk and meeting room. He may also request to access Electronic

Healthcare Records while outside the hospital. This movement may occur at different times.

Let's say John is a healthcare professional at the Muhimbili National Hospital in Dar es Salam, Tanzania. He has the privileges to access Anna's sensitive Electronic Healthcare Records (EHRs). He requested to access Anna's records at 8:00 am when in a meeting room with other healthcare professionals and again requested to access the records at 3:0pm while at the front desk and lastly he requested to access Anna's records at 8:00 pm, he while outside the hospital.

From the above scenario, let's say we consider location (of the subject) and time as our contextual attributes whereby

Subject_role = (Consultant, Specialist, Doctor, Nurse)
Location = (theatre, ward, pharmacy, office, front_desk, meeting_room, outside_hospital)
Time = (6:00am<time<5:00pm)

Note: Time indicates the duration where healthcare professionals can provide services to patients from outside (outpatients).

With these information then we can create a condition in an access control model by including these information and hence reducing the chances for breaching patient's confidentiality as well as security of the records. Example of the conditions may be

{subject: (can_access if subject_role = "doctor" ^ location = "theatre, ward, office" ^ time<5:00pm)}

Again as the state-of-art for the protection of EHRs in the healthcare environment, various access control models such as Role-Based Access Control (RBAC) [4], Team-Based Access Control (TMAC) [5] and Task-Based Access Control (TBAC) [6] have been used. With RBAC, access control decisions are often determined by the roles individual users take on as part of an organisation while TMAC and TBAC consider group roles and progression of the tasks respectively to control access to information. Due to the nature of the healthcare environment, these models and others are considered insufficient for the dynamic healthcare environment. The RBAC does not support the use of contextual attributes as it may result into role explosion while TMAC and TBAC are special configurations of RBAC. Therefore, with the identified promises of context in the dynamic healthcare environment, in this paper we look at how researchers other domains have attempted to define context in their own work as well as propose relevant contextual attributes for the domain.

Organisation of the paper: Section 2 provides a review of various definitions of context proposed by researchers from different domains. Section 3 discusses categories of context. Section 4 presents a review of context specifically for the healthcare environment while section 5 provides descriptions of contextual attributes. Section 6 provides discussion and future work

A. Aim of the Paper

Based on the survey performed on existing research literature, we intend to analyse how rich in contextual attributes the dynamic healthcare environment is and then propose relevant contextual attributes, with its associated subcategories, for the dynamic healthcare environment.

B. Methodology Used

For this study, research has been done through major electronic research databases (such as Medline, PubMed), scientific journals via their own sites as well as Web Search Engines (mostly Google Scholar). These resources were used to identify research published from different domains such as UbiComp that identify relevant contextual attributes for their domains.

Different themes were used to identify relevant papers for this study. The themes used include i. Context ii. Contextual attributes iii. Contextual attributes in healthcare iv. Context and electronic healthcare. To broaden our research references from the main papers were also studied.

II. CONTEXT

In this section we review various definitions of context that has been proposed by researchers from other domains and then evaluate them before proposing relevant contextual attributes for the dynamic healthcare environment.

The first and formal definition of context which enumerates context as location of use, identities of the nearby people and objects and changes to those objects over time was proposed by Schilit [7]. In a similar way, Ryan et al. [8] define context as user's location, environment, identity and time while Brown et al. [9] considered context as location, identities of the people around the user, orientation of the device, and time of the day, season of the year, temperature and so forth. Dey [10] enumerates context further as user's emotional state, focus of attention, location and orientation, date and time, objects and people in the user's environment.

Although these definitions provide examples of contextual attributes, it is difficult to apply any of them when we want to determine whether a type of information not listed in the definition is context or not. To solve the aforementioned problem, Dey and Abowd [11] provided a thorough definition which describes context as any information that can be used to characterise the situation of an entity where an entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves. Therefore from the definition, Dey and Abowd propose location, identity, time and activity as relevant contextual attributes.

Contextual attributes proposed by Ryan et al. [8] are considered as the consensus to those proposed by Dey and Abowd [11]. The only difference that exists in terms of contextual attributes between the two is that the latter proposed activity as contextual attribute instead of environment proposed by the former. Dey and Abowd [11]

argue that environment is a synonym for context and does not add anything in their research while activity will characterise the situation by indicating what is really occurring in such a situation.

III. Categories of Context

As highlighted in section 1, the principal aim of this paper is to propose relevant contextual attributes for the dynamic healthcare environment. The categorisation of context will help in identifying specific contextual attributes that need to be considered while providing healthcare professionals with dynamic levels of access to sensitive patient's EHRs.

Therefore, from section 2, different researchers have provided different categories of context. Dey and Abowd [11] while working in the UbiComp domain list location, identity, time and activity as important contextual attributes to the interaction between user and application while Schilit and Theimer [12] suggest location and identity as contextual attributes. Summary of the contextual attributes proposed by various researchers have been provided in table I.

TABLE I

SUMMARY OF CONTEXTUAL ATTRIBUTES

No.	Author	Contextual Attributes
1	Brown et al. [13]	Location, Time of the day, Season, Temperature, Identities of the people around the user, Orientation
2	Ryan et al. [8]	Location, Environment, Identity and Time
3	Dey [10]	User's emotional state, Focus of attention, Location of attention, Date and Time, Objects and People in user's environment
4	Dey and Abowd [11]	Location, Identity, Activity and Time.
5	Schilit and Theimer [12]	Location and Identity information
6	Coutaz et al. [14]	Location and Identity
7	Beresford [15]	Summarises Dey and Abowd's (2000) categories as Identity: identity of relevant entities. Location: geographical position of relevant entities Activity: activity or activities being performed Time: time period at which entities perform the activity
8	Kjeldskov and Skov [16]	Location, Time and Tasks.

Based on the literature review, as indicated in table 1, there is a huge variation on contextual attributes proposed by various researchers. Location, identity and time appear more compared to other attributes such as temperature and season. To resolve contextual attributes variation issue, Beresford [15], claims that, there are primary and secondary context whereby secondary context requires an association with one or more primary context to be meaningful. Therefore, for example, temperature is a secondary attribute associated with location while date of birth and address are secondary attributes associated with identity

IV. Context in the Healthcare Environment

For contextual attributes in the healthcare environment, Bricon-Souf and Newman [1] also argue that location, identity of the healthcare professionals and time are the most common attributes considered. However, from the literature review performed, we argue that the dynamic healthcare environment, which at the same time considered collaborative, is rich in context and there is lack of research to-date performed to identify contextual attributes specifically for the environment. For this paper identification of the contextual attributes together with their respective subcategories relevant for the dynamic healthcare environment is considered to be one of its contributions

Contrary to various contextual attributes proposed from other domains, for the dynamic healthcare environment we propose the use of resource rather than location. As EHRs are processed, stored (databases) and transmitted using EHISs then there is a need of using attributes of the database where these records are stored. The summary of the proposed contextual attributes and their sub categories has been provided in table II. In section 5 each proposed category together with its subcategory is briefly discussed.

V. Contextual Attributes: Descriptions

As presented in table II, contextual attributes in dynamic and collaborative healthcare environment can be categorised into four groups. These are attributes associated with the subject, time, activity and resource, whereby

- Subject involves individuals involved in the processing EHRs
- Activity: Includes activity or activities being performed
- Time: Is the time period at which entities perform the activity
- Resource: Is the storage space for Electronic Healthcare Records

As indicated in table III, Subject has various attributes associated with it such as Subject ID, Subject Name, Group ID, Group Name, Session Start Time, Session Start Date, Session Start Time and Date, IP Address, etc while Resource, as indicated in table IV, is associated with Resource Label, Resource Name, Row Label, View Label, Schema Label, Catalog Label, Database Label, Database Name, Column Name etc.

In addition to subject and resource's context, there is time and activity. Time is associated with Current Time, Current Date and Current Date and Time while Activity is associated with Activity ID, Activity Type and Activity Request Location.

With the presence of these and other attributes in the healthcare environment, which involves processing of sensitive patients information, combining with the fact that the more contextual attributes used the more fine-grained access control system becomes then there is a need of identifying specific contextual attributes for certain environment if EHRs need to be protected.

TABLE II

SUMMARY OF CONTEXTUAL ATTRIBUTES

Subject	**Time**	**Activity**	**Resource**
Subject ID	Current Time	Action ID	Resource Label
Subject Name	Current Date	Action Type	Resource Name
Group ID	Current Time Date	Action Request Location	Row Label
Group Name			Table Label
Session Start Time			View Label
Session Start Date			Schema Label
Session Start Time Date			Catalog Label
IP Address			Database Label
DNS Name			Column Name
Session Label			Table Name
User Current Location			View Name
User Allocated Location			Schema Name
			Catalog Name
			Database Name
			Any-row field value

TABLE III

SUBJECT ASSOCIATED ATTRIBUTES

ATTRIBUTE	DESCRIPTION
Subject ID	This is the numerical user-ID of the database subject performing the current database operation
Subject Name	This is the text user-name of the database subject performing the current database operation
Group ID	This is the numerical group ID of the database project performing the current database operation
Group Name	This is the test group name of the database subject performing the current database operation
Session Start Time	This is the local time the database subject started the current database session
Session Start Date	This is the local date the subject started the current database session
Session Start Date Time	This is the local date and time the database subject started the current database session
IP Address	This is the IP network address from which the current database subject started the current database session
DNS Name	This is the Domain-Name Service host name from which the database subject started the current database session
Session Label	This is the database session label at the time the database operation was submitted
User Current Location	As healthcare professionals tend to move over time, this is the current location where the user is.
User Allocated Location	This is the permanent location where the healthcare professional is allocated as his/her area of duty.

TABLE IV

RESOURCE ASSOCIATED ATTRIBUTES

ATTRIBUTE	DESCRIPTION
Resource Label	This is the sensitivity label of the database object currently being acted upon. Example of the resource label include: For row select: the label is row label, for schema open, label is schema label and for database-open the label is database-label
Resource Name	This is the fully specified name of the database object currently being operated upon. For table open, then the table name will be its associated resource name while for view-create its associated resource name is view-name.
Row Label	This is the sensitivity label of the database row currently being operated upon. This attribute only is associated with row-associated attributes such as row-insert, row-select, row-delete etc.
View Label	This is the sensitivity label of the database view currently operated upon. Like in row, this attribute is only associated with the database view such as view-open, view-create, view-drop operations.
Schema Label	This is the sensitivity label of the database schema currently being operated upon.
Catalog Label	is the sensitivity label of the database catalog currently being operated upon
Database Label	This is the sensitivity label of the database currently being operated upon
Column Name	This represent multi valued bag of specified column names of the database row currently being operated upon
Table Name	This represents the fully specified name of the database currently being operated upon
View Name	This is the full specified name of the database view currently being operated upon.
Schema Name	This is the fully specified name of the database catalog currently being operated upon.
Database Name	This is the name of the database currently operated upon.

VI. CONCLUSION AND FUTURE WORK

In this paper we have proposed contextual attributes, together with their respective subcategories, relevant for the dynamic healthcare environment. Contrary to other domains where location, identity and time appear to be more important, in healthcare we propose the use of these three attributes together with resource rather than location. The reason behind our selection of resource rather than location is that location is basically associated with the subject or resource as it cannot stand on its own without resource or subject in place. Generally speaking, location is a secondary attribute to subject and resource. In addition, resource is more important in healthcare as it is where patient's Electronic Healthcare Record is stored.

As context tends to affect security, together with difficulty in defining context, then the proposed contextual attributes for the dynamic healthcare environment will be used as a guideline while identifying specific contextual attributes for the Tanzania's healthcare environment. The approach being adopted for our main research is by adding specific contextual attributes, from the Tanzania's healthcare environment, into the Role Based Access Control model while developing a dynamic context-aware access control model for securing EHRs in Tanzania. As for our future work we intend to propose appropriate contextual attributes, specific for the Tanzania's healthcare workflow, after conducting an in-depth interview and survey with healthcare professionals in the area.

REFERENCES

[1] N. a. Bricon-Souf and C. R. Newman, "Context awareness in healthcare: A Review.," *International Journal of Medical Informatics*, vol. 76, pp. 2-12, 2007.

[2] R. Kuhn, Coyne, E. J., and Weil, T. R., "Adding Attributes to Role Based Access Control," *IEEE Computer Society*, 2010.

[3] Cisco, "The Cisco Context-Aware Healthcare Solution," 2009.

[4] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer*, vol. 29, pp. 38 - 47, 1996.

[5] R. K. Thomas, "Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments," *RBAC '97 Proceedings of the second ACM workshop on Role-based access control*, 1997.

[6] R. K. Thomas and R. S. Sandhu, "Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management," 1997.

[7] W. N. Schilit, "A System Architecture for Context-Aware Mobile Computing," in *Graduate School of Arts and Sciences*, vol. PhD: Columbia University, 1995.

[8] N. Ryan, J. Pascoe, and D. Morse, "Enhanced Reality Fieldwork: the Context-Aware Archaeological Assistant," in *Computer Applications in Archaeology*, 1997.

[9] P. J. Brown, J. D. Bovey, and X. Chen, "Context-aware Applications: from the Laboratory to the Marketplace," *IEEE Personal Communications*, vol. 4, pp. 58-64, 1997.

[10] A. K. Dey, ""Context-Aware Computing: The CyberDesk Project"," *AAAI 1998 Symposium on Intelligent Environments*, pp. 51-54, 1998.

[11] A. K. Dey and G. D. Abowd, "Towards a better Understanding of Context and Context Awareness," presented at Proceedings of the 2000 Conference on Human Factors., 2000.

[12] B. N. Schilit, Adams, N., Want, R., "Context-Aware Computing Applications," *IEEE Workshop on Mobile Computing and Applications*, 2004.

[13] P. J. Brown and J. D. Bovey and X. Chen, "Context-aware Applications: from the Laboratory to the Marketplace," *IEEE Personal Communications*, vol. 4, pp. 58-64, 1997.

[14] J. Coutaz, Crowley, J. L., Dobson, S., and Garlan, D., "Context is Key," *Communications of the ACM*, vol. 48, pp. 49-53, 2005.

[15] A. R. Beresford, "Location privacy in Ubiquitous Computing," University of Cambridge 2005.

[16] J. Kjeldskov, and Skov, M. B., "Exploring Context-Awareness for Ubiquitous Computing in the healthcare domain.," *Pers Ubiquit Compu*, pp. 549-562, 2007.

Context and Access Control for Healthcare

Zanifa Omary, Fredrick Mtenzi
School of Computing
Dublin Institute of Technology
Kevin Street, Dublin 8, Dublin, Ireland
Zanifa.Omary@dit.ie, Fredrick.Mtenzi@dit.ie

Bing Wu
School of Computing
Dublin Institute of Technology
Kevin Street, Dublin 8, Dublin, Ireland
Bing.Wu@dit.ie

ABSTRACT

Electronic healthcare, while exciting and promising, presents many challenges to patients' Electronic Healthcare Records (EHRs) such as Privacy and Security. Some accumulating evidences show that adding appropriate context in an access control model can help improve the security of EHRs. Contrary to such benefits, researchers in the healthcare environment are yet to harness it as they keep on adopting context proposed in other domains such as Ubiquitous Computing. This act, in turn, reduces the rate of protection of EHRs as wrong contextual information results into wrong access control and hence insecure EHR systems. In this paper we analyse how rich in terms of context the healthcare environment is and then propose relevant contextual attributes for the domain. Moreover we examine the usage of proposed contextual attributes into the existing access control models.

Keywords: Context, Access Control, Electronic Healthcare Record

I.INTRODUCTION

The shift in the healthcare domain from paper-based towards Internet-related healthcare activities often referred to as *"e-healthcare"* is dramatic and considered as the most significant development in the healthcare domain. Although this change is considered exciting and promising, it presents many challenges to patients' EHRs such as privacy and security. While these challenges exist in other domains as well, in the healthcare environment they are considered critical due to the sensitivity of patients' information that is being processed, stored and transmitted using EHR systems. The security breaches towards EHR systems may result into patients' harm, social embarrassment or prejudice and may even affect patient's insurability. Despite the presence of association between these two challenges, privacy and security, in this paper our main focus will be on security.

Current solutions to this problem (mostly built on Role-Based Access Control (RBAC) which uses job functions to control access) do not address the intricate security requirements of healthcare applications. The healthcare industry requires dynamic, context-aware access control to provide more precise and fine-grained authorisation policies for any application. Some accumulating evidences show that adding appropriate context in an access control model can help improve the security of EHRs by maintaining patients' privacy and confidentiality. Moreover, context can also be used to introduce and extend the required dynamism in the whole healthcare sector to reflect, for example, changes in the working conditions, staffing levels, policies and even types of ailment being treated within the healthcare sector.

Contrary to such benefits of context when appropriately used, researchers in the healthcare environment are yet to harness it as they keep on adopting contextual attributes proposed in other domains. This act, in turn, reduces the rate of protection of EHRs as wrong contextual information results into wrong access control and hence insecure EHR systems. In this paper we intend to analyse how rich in terms of context the

healthcare environment is and then propose relevant contextual attributes for the domain. Furthermore we examine the usage of proposed contextual attributes into the existing access control models. To achieve this, research has been conducted through major electronic research databases (such as Medline, PubMed), Scientific Journals via their own sites as well as Web Search Engines (mostly Google Scholar). These resources were used to identify research published from different domains that identify relevant contextual attributes for their domains. Different themes, such as context, contextual attribute, contextual information, contextual attributes in healthcare and context and electronic healthcare were used to identify relevant papers for this study. To broaden our research references from the main papers were also studied.

The rest of this paper is organised as follows. Section II provides background information regarding context followed by the review of various definitions of context in section III. Section IV provides a discussion on the related work in relation to context. Section V presents an analysis of contextual attributes specifically for the healthcare environment while section VI presents a discussion on access control models for the healthcare environment taking into consideration the presence of proposed contextual attributes. Section VII provides conclusion and future work.

II.BACKGROUND CONTEXT

For numerous years, the concept of context has been studied by philosophers, linguists, psychologists, and recently by computer scientists. Its usage, in the Computer Science field, is growing rapidly in various applications and domains ranging from Information Retrieval, Reasoning in Artificial Intelligence (AI), Ontology, to Knowledge Representation [1]. Within each domain, context has been interpreted in a certain way that is well-suited for their goal and hence making it an elusive concept to define [2]. In this section we provide the background information regarding context by using a scenario. Therefore before delving further into it and discuss the benefits of context in the healthcare environment, which spans from patients to healthcare professionals, let's consider its usage in the following scenario.

Within a hospital, a healthcare professional can move between theatre, ward, pharmacy, office, front desk and meeting room. He may also request to access EHRs while outside the hospital using his mobile device. This movement may occur at different times during a day.

Let's say John is a healthcare professional at Muhimbili National Hospital in Dar es Salam, Tanzania. He has the privileges to access and modify Anna's sensitive EHRs. He, first, requested to access Anna's records at 8:00 a.m. when in a meeting room with a Consultant and again requested to access the same records at 3:00p.m while at the front desk and lastly he requested to access Anna's records at 8:00 pm, while he is in his private office outside the hospital.

The above scenario can be summarised as shown in table 1 where resource for all the three scenarios is Anna's EHRs.

Table 1: Context and Access to patient's information

Subject	Location	Time
John	Meeting Room	8:00 am
John	Front Desk	3:00 pm
John	Private Office	8:00 pm

Let's say we consider traditional access control models such as RBAC [4], which uses job function, to control access to patients' records. With this model then John will be able to access records in all the scenarios as only his role will be considered while making access decisions. Consequently, if we take into consideration new models such as Attribute Based Access Control (ABAC) [5], which considers dynamic healthcare professionals attributes such as current location and time of the day, then John's level of access to the records will change. Table 2 presents contextual attributes; these are subject role, location, time and resource; that may be used to control access to patient's records.

Table 2: Healthcare environment contextual attributes

Subject_role=(Consultant,Specialist,Doctor,Nurse)
Location = (theatre, ward, pharmacy, office, front_desk, meeting_room, outside_hospital)
Time = (6:00am <time< 5:00pm)
Resource = (patients' records)

To harness the presence of context then we can create a condition in an access control model by

including contextual attributes. This will reduce chances for breaching patient's confidentiality as well as help in maintaining patients' privacy. Table 3 shows access control condition with contextual information. The condition states that a doctor can access sensitive patient's records between 6:00 a.m. and 5:00 p.m. while in the theatre or ward. This condition will limit access when a doctor requests to access records while in the front desk or his office.

Table 3: Access control condition with contextual information

{Subject: (can_access patient record if subject_role = "doctor" ^ location = "theatre, ward" ^ 6:00a.m. <time<5:00pm)}

From the above scenario then benefits of context in the healthcare environment can be summarised as follows.

For the patients, the appropriate usage of contextual information is expected to enhance the security of patients' records and help maintaining patients' privacy. That is, it provides healthcare professionals with dynamic levels of access to the records depending on the captured contextual information. To elaborate this, consider, for example, two healthcare professionals requesting access to Anna's EHRs; the first healthcare professional is requesting to access records using his mobile device while he is in his private office (outside the hospital) and another professional is in the ward (within the hospital). While considering location, which is contextual information, before providing access, then these two professionals will be provided with two different levels of access to the records as the latter may be denied access or granted access to basic information only while the other being given full access.

For the healthcare centre, context tends to improve operational efficiency by integrating real time contextual information, such as location, status of medical equipment and staff, into the healthcare workflow [6]. As a result of this, context then enhances quality of patient care, increases staff efficiency while helping the healthcare organisation to manage capital and operational costs. Yet again for patients within the healthcare centre, context enables access to environmental information, such as temperature or humidity, to provide an optimal patient experience [6]. In section III a review of various definitions of context proposed by researchers from different applications and domains will be provided.

III.CONTEXT

In this section we review various definitions of context that has been proposed by researchers from different applications and domains and then we evaluate them before proposing a general definition of context that will be considered relevant for the rest of this paper. These definitions will later be referred while proposing appropriate contextual attributes for the healthcare environment.

Although the word context has been used for a number of years in many scientific descriptions, literature essays and in philosophical discourses, there is no single agreed definition which is yet available, though there is a serious ongoing effort to make a precise working definition of context [2, 7].

Oxford English Dictionary (OED) refers context to as the merging together of circumstances that form an event. To emphasise a common social usage of context, OED [8] includes a quotation from R. Cobden speeches *"I wish honourable gentlemen would have the fairness to give the entire context of what I did say, and not pick out detached words"*. Consider the following event as an example of the usage of the entire context in the healthcare environment "Doctor John will be attending a consultation meeting in room G20 from 10:00 a.m. to 12:00 noon".

For the Computer Science field, the first and formal definition of context which enumerates context as location of use, identities of the nearby people and objects and changes to those objects over time was proposed by Schilit [9]. In a similar way, Ryan et al. [10] define context as user's location, environment, identity and time while Brown et al. [11] considered context as location, identities of the people around the user, orientation of the device, and time of the day, season of the year, temperature. Dey [12] enumerates context further as user's emotional state, focus of attention, location and orientation, date and time, objects and people in the user's environment.

Although most of these definitions, except OED's, propose contextual attributes instead of defining what context is, it is therefore difficult to apply any of them when we want to determine whether a type of information not listed in the definition is context or not. To solve the aforementioned problem, Dey and Abowd [13] provided a thorough definition which describes

context as any information that can be used to characterise the situation of an entity where an entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves. Therefore from the definition, Dey and Abowd propose location, identity, time and activity as relevant contextual attributes.

Contextual attributes proposed by Ryan et al. [10] are considered as the consensus to those proposed by Dey and Abowd [13]. The only difference that exists between the two is that the latter proposed activity as contextual attribute instead of environment proposed by the former. Dey and Abowd [13] argue that environment is a synonym for context and does not add anything in their research while activity will characterise the situation by indicating what is really occurring in such a situation. However, as the intention of this section is to provide a generic definition of context only then we adopt a definition proposed by OED which briefly refers context to as the merging together of circumstances. This definition indicates what context is without paying much attention to the presence of contextual attributes in order to define context. The appropriate contextual attributes for the healthcare domain will be provided in section V.

IV.RELATED WORK

As discussed in section I, the principal aim of this paper is to propose relevant contextual attributes together with their extended subcategories for the healthcare environment. In order to accomplish it, in this section we review contextual attributes (information) that has been proposed by researchers in various domains and applications. This analysis will help in identifying specific contextual attributes that need to be considered while making access decisions in the healthcare environment.

Moreover, as discussed in section II, researchers in various domains and applications have provided different contextual attributes depending on their goals and the domain that they are working in. In 1993, Weiser [14], who is widely considered as the father of UbiComp, introduced situation as one of the important contextual attributes while working at the Xerox Palo Alto Research Center (PARC) laboratory. Since then situation has been widely used and applied in various domains.

Inspired by the vision of UbiComp and their own experiences, Schilit et al. [15] suggested situation and location as important contextual attributes in Mobile Computing. Their reason behind suggesting these two related attributes is that computer users may move from one location to another joining and leaving groups of people and frequently interacting with computers while in changing social situations.

Bertino et al. [16] have proposed time while developing a time-based authorisation model. This model was later generalised and extended to role-hierarchies, separation of duty and cardinality constraints; Generalised Temporal Role-Based Access Control (GTRBAC) [17], in which the notion of time has been considered only.

Dey and Abowd [13] while working in the UbiComp domain and following closely Weiser's work list location, identity, time and activity as important contextual attributes to the interaction between user and application. Moreover, Schilit and Theimer [18] suggest location and identity as contextual attributes while Chandaran et al. [19] imply time and location constraints. Table 4 provides a summary of contextual attributes proposed by researchers in various domains.

Table 4: Summary of Contextual Attributes (Source: Author)

No.	Author	Contextual Attributes
1.	Weiser [14]	Situation
2.	Schilit et al. [15]	Location and situation
3.	Brown et al.[20]	Location, Time of the day, Season, temperature, Identities of the people around the user, orientation
4.	Ryan et al. [21]	Location, Environment, Identity and Time
5.	Bertino et al.[16]	Time
6.	Dey [12]	User's emotional state, Focus of attention, Location of attention, Date and Time, Objects and People in user's environment
7.	Dey and Abowd [13]	Location, Identity, Activity and Time.
8.	Schilit and Theimer [18]	Location and Identity information
9.	Coutaz et al. [22]	Location and Identity
10.	Beresford [23]	Identity, Location,

		Activity and Time
11.	Chandaran et al. [19]	Location and Time
12	Kjeldskov and Skov [24]	Location, Time and Tasks.
13.	Tahir [25]	Purpose, location and time

As depicted in table 4, there is a huge variation on contextual attributes proposed by various researchers. Location, identity and time appear more compared to other attributes such as temperature and season. From the review done for this paper, out of 13 papers reviewed for the contextual attributes, 10 propose location, 6 propose identity and 8 suggests time while 4 used all of the three attributes. To resolve contextual attributes variation issue, Beresford [23], claims that, there are primary and secondary context whereby secondary context requires an association with one or more primary context to be meaningful. Therefore, for example, temperature is a secondary attribute associated with location while date of birth and address are secondary attributes associated with identity. Based on Beresford's claim, various researchers [26, 27] have used these four attributes regularly which made them popular than others.

V.CONTEXT IN THE HEALTHCARE ENVIRONMENT

For contextual attributes in the healthcare environment, Bricon-Souf and Newman [1] also argue that location, identity of the healthcare professionals and time are the most common attributes considered. However, from the review of literature performed, in this paper we argue that the healthcare environment, which at the same time considered collaborative, is rich in context and there is a lack of research to-date performed to identify contextual attributes specifically for the domain.

To support our argument on the existence of various context in the healthcare domain, Beznosov [28] proposed affiliation, role, location, time and relationship as requirements for access control in the United States healthcare domain. Tahir [25] who engrossed to know not only who, when and from where but also for what purpose an access request is made introduced new contextual attributes from the common ones. He introduced purpose in his flexible access control model referred to as Context-Role Based Access Control (C-RBAC). The C-RBAC model, which aims at preserving patient's privacy, extends the traditional RBAC model not only with location, identity and time but also with the notion of purpose.

Contrary to the four common contextual attributes, which are location, identity, time and activity, proposed and used in various applications and domains, in the healthcare environment we propose the use of the subject, activity, resource and time (which is environmental attribute) as shown in figure 1. Generally speaking, we associate location and identity as subcategories for the Subject attribute. Apart from that, we add a Resource as a category that need to be considered while controlling access. There are several reasons behind this substitution of contextual attributes.

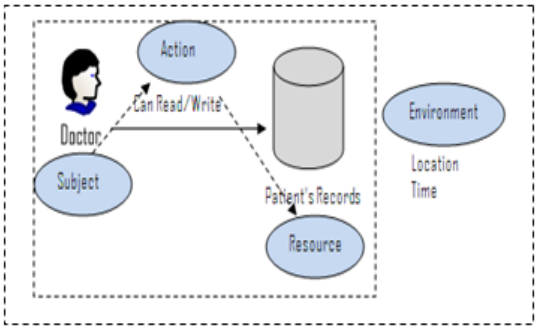


Figure 1: **Context in healthcare domain (Source: Author)**

For the resource, as EHRs are processed, transmitted and stored (in databases) using EHR systems, then there is a need of using attributes of the resource while controlling access to such sensitive information. For the location which is referred to as where the user is accessing information services from, then we argue that location cannot stand on its own without the presence of the healthcare professional in order to be considered meaningful in the healthcare sector.

Consider a policy which states that "a nurse should have access to medical record of the patient if the nurse is currently working on the same "floor" as the patient". With this policy, we argue that location is binded to both patient and a nurse, therefore from Beresford's categorisation; location is just a secondary attribute of the subject.

The four contextual attributes in the healthcare environment are defined as follows:

- Subject contains attributes that refers to an individual requesting access to patient's EHRs

- Activity: refers to action that Subject is requesting to perform to the resource
- Time Is the time period at which healthcare profesional is requesting to perform an activity to the resource.
- Resource: For the healthcare environment, EHRs are the resource. We can extend to include charactristics of the database where these records are stored.

As indicated in Figure 2, these attributes can be extended with various subcategories. Subject, for example, can be extended into Subject ID, Subject Name, Group ID, Group Name, Session Start Time, Session Start Date, and the combination of Session Start Time and Date, IP Address, etc while Resource can be extended with Resource Label, Resource Name, Row Label, View Label, Schema Label, Catalog Label, Database Label, Database Name, Column Name etc.

In addition to subject and resource's subcategories, there is time and activity. Time is associated with Current Time, Current Date and the combination of Current Date and Time while Activity is associated with Activity ID, Activity Type and Activity Request Location.

With the presence of these attributes and their subcategories in the healthcare domain, which involves processing of sensitive patients' information, combining with the fact that the more contextual attributes used the finer-grained access control system becomes then there is a need of identifying specific contextual attributes for certain environment if EHRs need to be protected. However to avoid ambiguities associated with access control, researchers need to provide description for each contextual attribute and their subcategories [29]. In section VI we analyse access control models based on their applicability in the healthcare domain as well as the presence of proposed contextual attributes in those models.

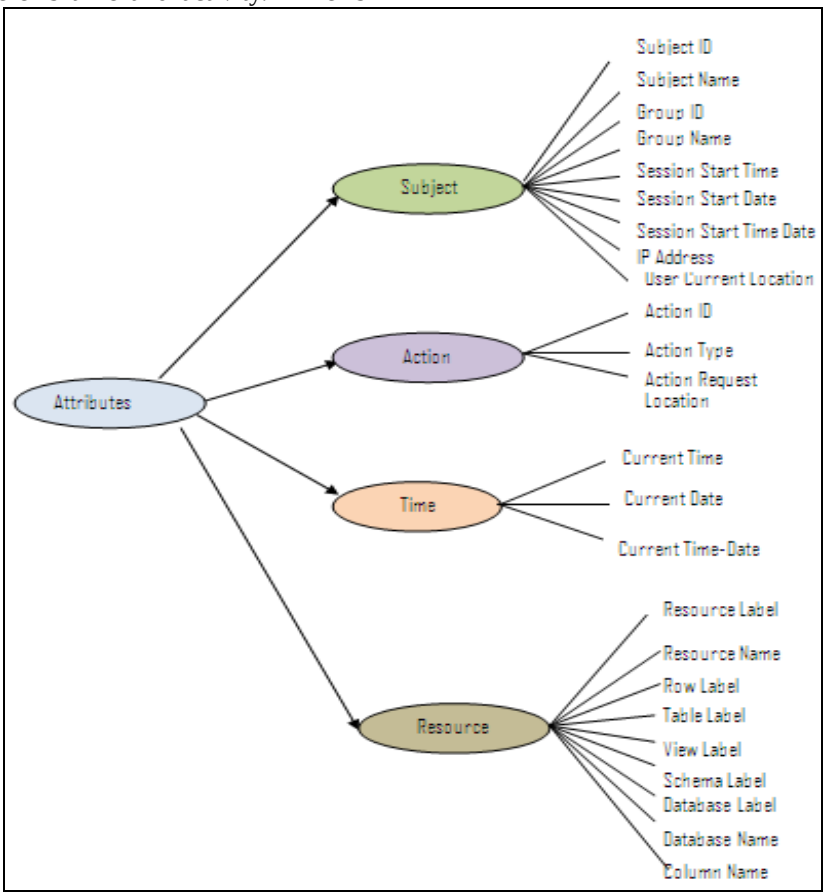


Figure 2: Extended Contextual Attributes (Source: Author)

VI. ACCESS CONTROL MODELS

In computing, access control refers to security features that control which principals (can be persons, processes or machines) have access to which resources. To achieve this, various access control models, such as Discretionary Access Control (DAC) [30], Mandatory Access Control (MAC) [30], Role-Based Access Control (RBAC) [4] and Attribute-Based Access Control (ABAC) [5], have been developed.

The traditional access control models, such as DAC and RBAC, are usually static as they don't take into consideration contextual information while making access decisions. However this act is considered inadequate for specifying access control needs of complex real world applications such as in the healthcare domain. In this section we analyse applicability of various access control models for the healthcare domain.

VI.I. DISCRETIONARY ACCESS CONTROL (DAC)

According to the Trusted Computer System Evaluation Criteria, TCSEC [30], DAC is a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The control is discretionary in the sense that, DAC leaves certain amount of access control to the discretion of the object's owner or anyone else who is authorised to control object's access [31].

With DAC model, user who created the object has all the permissions about it and also can delegate his/her permissions to others. The DAC policy tends to be very flexible and has been widely used in commercial and government sectors. Despite its widely use, we consider this model as inappropriate for the healthcare domain as healthcare professionals create patient records but they are not considered as the data owners and delegation can result into the breach of patient's privacy and information security.

VI.II. MANDATORY ACCESS CONTROL (MAC)

The TCSEC [30] defines MAC as a means of restricting access to objects based on the sensitivity of information contained in and the formal authorisation i.e. clearance of subjects to access information of such sensitivity. With MAC, security policy is centrally controlled by a security administrator and hence users do not have an ability to override the policy. The MAC policy is widely applied in military information systems where the individual data owner cannot decide who has the *Top Secret Clearance* nor can the owner change the classification of the object from for example *Top Secret* to *Secret*.

In relation to its use in the healthcare domain, like DAC, MAC is also considered inappropriate. For the healthcare environment, in case of an emergency, healthcare professionals require an ability to override security policies in order to provide care to patients. As previously discussed, this is not possible in MAC as only security administrator is allowed to make changes and therefore hence making this model inappropriate for the healthcare environment.

VI.III. ROLE-BASED ACCESS CONTROL (RBAC)

In many organisations, users do not own information which they created or are allowed access to [32, 33]. For such organisations, corporation/agency is the actual "owner" of the system objects as well as programs that process it and control is basically based on the user's functions rather than data ownership [32]. When using job functions that an individual user take as part of the organisation to control access, then the model being considered is RBAC [34].

In RBAC, permissions are associated with roles and users are assigned to appropriate roles [4, 34]. This assignment greatly simplifies security administration [4]. Consider for example, if within a hospital, an individual user has been moved from staff nurse to specialist nurse then using RBAC, the individual user can be assigned to a new role and removed from the old one whereas in the absence of RBAC, the user's old permissions would have to be individually revoked and new permissions would have to be granted. RBAC is also considered useful as it supports review of permissions assigned to users.

Despite its various benefits, RBAC has frequently been criticised for its difficulty in setting up an initial role structure also known as role engineering and its inflexibility in rapidly changing environments like healthcare [35]. A pure RBAC solution may provide inadequate support for dynamic contextual attributes such as current location, current date and time of the day. Capturing context using RBAC would mean defining large set of roles for each possible contextual attribute. Moreover, to define fine-grained permissions would also create large sets of permissions and hence resulting into role explosion [35]. To make RBAC simple and

flexible for the dynamic environments like healthcare, this widely used model need to be enhanced with contextual attributes. Using XACML ABAC [36], for example, role is defined as subject_role and considered as contextual information. Various researchers [17, 19, 25, 37-39] have extended RBAC model with contextual attributes such as environmental roles, location, location and time, location and location, time and purpose respectively.

VI.IV.TEAM-BASED ACCESS CONTROL (TMAC)

TMAC is an approach of applying RBAC in collaborative environments where an activity is best accomplished through teams [40]. Alotaiby and Chen [37] present a TMAC extension model, called TMAC04, built on RBAC which efficiently represents teamwork in the real world. The TMAC04 model allows certain users to join a team based on their existing roles in an organisation within limited context and new permission to perform the required work.

In relation to the identified need of contextual attributes which are considered important for providing fine-grained access control in a dynamic healthcare environment, TMAC doesn't bring anything new from RBAC's perspective.

VI.V. TASK-BASED ACCESS CONTROL (TBAC)

Contrary to other access control models where access rights are granted to subjects, with TBAC access rights are granted to tasks in steps related to the progress of the tasks [41]. Based on its provision of access rights to tasks, this model is considered as a dynamic access control technique [42]. TBAC is also considered to be suitable for automated processes where activities of the tasks cross computer boundaries. Despite being acknowledged as a dynamic access control technique, the use of tasks adopted by TBAC is regarded as a specific configuration of RBAC where context (tasks) can be viewed as constraints.

VI.VI. ATTRIBUTE-BASED ACCESS CONTROL (ABAC)

This model, which also referred to as Policy or Claims Based Access Control, is quite the opposite of RBAC. It was introduced to address issues associated with RBAC model such as role explosion which occurs when contextual attributes are captured and defined in RBAC and hence resulting in to thousands of roles associated with thousands of permissions.

ABAC's central idea is to use individual user's attributes to provide access decisions [5, 35]. ABAC policy specifies which claim(s) need to be satisfied in order to grant access to the resource. Any user who can prove such a claim is granted access. Consider, for example, an ABAC policy contains the claim *"above 18",* then any person who can prove this claim is granted access. Among the attributes associated with ABAC include: the subject who is demanding access, the action which the subject want to perform, the resource being accessed and the environment or context in which access is requested. These four attributes, which resembles to what we have proposed for the healthcare environment are considered as general attributes which contain other attributes within as shown figure 2.

Contrary to RBAC which is considered inappropriate for dynamic environments like healthcare as it does not support the use of context and capturing context may result in to role explosion, ABAC is considered to be flexible as it does not require separate roles for relevant sets of subject attributes and rules can be implemented quickly to cater for the changing needs [5]. In general, ABAC's approach made it easy to include context in the access control decisions. As a trade-off to its flexibility, this model suffers from complexity associated with the number of cases that need to be considered for the model as for *n* attributes or conditions using attributes, there are 2^n possible combinations. The model also requires an agreement on the meaning of attributes [5].

From these access control models and others, Role-Based Access Control has proved to be more popular and is considered as an efficient way of assigning access rights to users while at the same time ensuring data security. Despite its popularity, RBAC is criticised for its difficulty in setting up an initial role structure and for its inflexibility in rapidly changing environments [35]. To cater for the dynamic environments like healthcare which involves processing, transmitting and storing sensitive EHRs, RBAC needs to be enhanced with contextual attributes such as subject's current location, current date and time of the day. Moreover from analysis of access control models performed, there is no single access control model which has been developed and comprises all contextual attributes rather it includes part such as location and/or time [25]. In this paper, we argue

that in order to ensure security of patient's information all appropriate contextual attributes should be used while designing and developing and access control model as wrong or partial contextual attributes means inappropriate access control and hence threatening the security of patients' information.

VII. CONCLUSION AND FUTURE WORK

In this paper we have analysed how rich in terms of context the healthcare environment is and then we have propose relevant contextual attributes for the domain. Moreover we have examined the usage of proposed contextual attributes into the existing access control models. Contrary to other domains where location, identity, activity and time appear to be more important, in healthcare domain we have proposed the use of subject, activity, time and resource. Generally speaking, in this paper we have associated location and identity as subcategories or secondary categories for the main Subject attribute. For the case of location for example, for it to be meaningful it needs to be associated with the Subject. In addition we have included resource which is considered to be more important in healthcare as it is where patient's Electronic Healthcare Record is stored.

REFERENCES

1. N. a. Bricon-Souf and C. R. Newman, "Context awareness in healthcare: A Review.," International Journal of Medical Informatics, vol. 76, pp. 2-12, 2007.
2. K. Wan, "A Brief History of Context," IJCSI International Journal of Computer Science Issues, vol. 6, 2009.
3. R. Kuhn, Coyne, E. J., and Weil, T. R., "Adding Attributes to Role Based Access Control," IEEE Computer Society, 2010.
4. R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models," Computer, vol. 29, pp. 38-47, 1996.
5. A. H. Karp, H. Haury, and M. H. Davis, "From abac to zbac: The evolution of access control models," Technical report, HP Laboratories Palo Alto 2009.
6. Cisco, "The Cisco Context-Aware Healthcare Solution," C. Systems, Ed., 2009.
7. A. K. Dey, "Understanding and Using Context," Personal and Ubiquitous Computing Journal, vol. 5, 2001.
8. OED, "Oxford English Dictionary," Oxford University Press, 2011.
9. W. N. Schilit, "A System Architecture for Context-Aware Mobile Computing," in Graduate School of Arts and Sciences, vol. PhD: Columbia University, 1995.
10. N. Ryan, J. Pascoe, and D. Morse, "Enhanced Reality Fieldwork: the Context-Aware Archaeological Assistant," in Computer Applications in Archaeology, 1997.
11. P. J. Brown, J. D. Bovey, and X. Chen, "Context-aware Applications: from the Laboratory to the Marketplace," IEEE Personal Communications, vol. 4, pp. 58-64, 1997.
12. A. K. Dey, ""Context-Aware Computing: The CyberDesk Project"," AAAI 1998 Symposium on Intelligent Environments, pp. 51-54, 1998.
13. A. K. Dey and G. D. Abowd, "Towards a better Understanding of Context and Context Awareness," presented at Proceedings of the 2000 Conference on Human Factors., 2000.
14. M. Weiser, "Some Computer Science Issues in Ubiquitous Computing," Communication of the ACM, vol. 36, pp. 74-84, 1993.
15. B. Schilit, N. Adams, and R. Want, "Context-Aware Computing Applications," presented at WMCSA 1994, 1995.
16. E. Bertino, C. Bettini, E. Ferrari, and P. Samarati, "An access control model supporting periodicity constraints and

temporal reasoning," ACM Transactions on Database Systems (TODS), vol. 23, pp. 231-285, 1998.

17. E. Bertino, B. Catania, M. L. Damiani, and P. Perlasca, "GEO-RBAC: a spatially aware RBAC," 2005.

18. B. N. Schilit, Adams, N., Want, R., "Context-Aware Computing Applications," IEEE Workshop on Mobile Computing and Applications, 2004.

19. S. Chandran and J. B. D. Joshi, "LoT-RBAC: A location and time-based RBAC model," Web Information Systems Engineering–WISE 2005, pp. 361-375, 2005.

20. P. J. Brown, J. D. Bovey, and X. Chen, "Context-aware applications: from the laboratory to the marketplace," Personal Communications, IEEE, vol. 4, pp. 58-64, 1997.

21. N. S. Ryan, J. Pascoe, and D. R. Morse, "Enhanced reality fieldwork: the context-aware archaeological assistant," 1998.

22. J. Coutaz, Crowley, J. L., Dobson, S., and Garlan, D., "Context is Key," Communications of the ACM, vol. 48, pp. 49-53, 2005.

23. A. R. Beresford, "Location privacy in Ubiquitous Computing," University of Cambridge 2005.

24. J. Kjeldskov, and Skov, M. B., "Exploring Context-Awareness for Ubiquitous Computing in the healthcare domain.," Pers Ubiquit Compu, pp. 549-562, 2007.

25. M. N. Tahir, "C-RBAC: Contextual role-based access control model," Ubiquitous Computing And Communication Journal, vol. 2, 2007.

26. M. Baldauf, S. Dustdar, and F. Rosenberg, "A survey on context-aware systems," International Journal of Ad Hoc and Ubiquitous Computing, vol. 2, pp. 263-277, 2007.

27. F. L. Gandon and N. M. Sadeh, "Semantic web technologies to reconcile privacy and context awareness," Web Semantics: Science, Services and Agents on the World Wide Web, vol. 1, pp. 241-260, 2004.

28. K. Beznosov, "Requirements for access control: US Healthcare domain," 1998.

29. Z. Omary, F. Mtenzi, and B. Wu, "Context for Securing EHRs in a Dynamic Healthcare Environment."

30. DoD, "Trusted Computer System Evaluation Criteria," December 1985.

31. D. F. Ferraiolo, V. C. Hu, and D. R. Kuhn, "Assessment of Access Control Systems," 2007.

32. M. A. C. Dekker, "Flexible access control for dynamic collaborative environments," 2009.

33. D. F. Ferraiolo and D. R. Kuhn, "Future directions in role-based access control," 1996.

34. D. Ferraiolo, D. R. Kuhn, and R. Chandramouli, Role-based access control: Artech House Publishers, 2003.

35. D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding Attributes to Role-Based Access Control," Computer, vol. 43, pp. 79-81, 2010.

36. A. Anderson, "Core and hierarchical role based access control (RBAC) profile of XACML v2. 0," OASIS Standard, 2005.

37. F. T. Alotaiby and J. X. Chen, "A model for team-based access control (TMAC 2004)," 2004.

38. C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati, "Supporting location-based conditions in access control policies," 2006.

39. M. J. Covington, W. Long, S. Srinivasan, A. K. Dev, M. Ahamad, and G. D. Abowd, "Securing context-aware applications using

environment roles," 2001.

40. R. K. Thomas, "Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments," 1997.

41. R. K. Thomas and R. S. Sandhu, "Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management," Database Security, vol. 11, pp. 166-181, 1998.

42. O. Moonian, K. K. Khedo, S. Cheerkoot-Jalim, R. Doomun, S. D. Nagowah, and Z. Cadersaib, "HCRBAC _ An Access Control System for Collaborative Context-Aware HealthCare Services in Mauritius," Journal of Health Informatics in Developing Countries, 2008. 2: 10-21.

Dynamic Context Aware Access Control Model for the Areas with Shortage of Healthcare Professionals

Zanifa Omary[1], Fredrick J. Mtenzi[2], Bing Wu[3]
School of Computing
Dublin Institute of Technology
Kevin Street, Dublin 8, Dublin, Ireland
{Zanifa.Omary[1], Fredrick.Mtenzi[2], Bing.Wu[3]}@dit.ie

Abstract: **Although access control is considered as a well known and used concept in various domains, its usage for the areas with the limited number of professionals is considered minimal. In this paper we present a dynamic context-aware access control model by extending the traditional role-based access control model with location, and other, information. The presented model aims at improving security of patient's Electronic Healthcare Records (EHRs) for the areas with the shortage of healthcare professionals.**

Introduction

In recent years, various domains, ranging from Insurance[1] to Ubiquitous Computing [2], have been using location, and other, information to provide context-specific services to their customers. For Ubiquitous Computing, for example, location information has been widely used to remotely monitor elderly anytime anywhere and provide tailored services for each person based on the person's condition. An example of such a mobile health monitoring system for the elderly is proposed by [3].

Apart from monitoring elderly from the comfort of their homes, which is much common in Ubiquitous Computing [4], in the healthcare domain, location information is mainly used to control access to sensitive records. This main role of location information, to healthcare domain, can be categorised further into three subtasks, these are: controlling access to sensitive healthcare information [5], establishing the level of trust to the domain and deriving emergency level of access [6].

In order to control access to sensitive patient's information, an access control policy should be defined in such a way that it takes into

consideration location and other contextual information while making access control decision [7]. An example of such a policy that aims to control access to the records would be, **"a nurse should have access to the sensitive records of the patient if s/he is scheduled on the same department as to where the patient is admitted and no bigger role than nurse is currently working in the department".**

For the establishment of the level of trust to the domain, a reasonable policy should deny access to sensitive patient's information to anyone trying to access records from untrustworthy areas. Furthermore, a realistic policy for the healthcare domain should allow different levels of access to the records depending on the contextual information gathered. Let's say for example, two professionals with the same role (nurse, for example), one in the reception area and the other in the ward, should have different levels of access to the patient's records.

With its numerous uses, location information, which is defined as to where the user is accessing information services from [8], is considered as one of the powerful and yet useful concepts in various domains [9]. This paper presents a dynamic context aware access control model that dynamically grants permission to users based on current context. The proposed mechanism, which is aimed at improving security of patient's EHRs in areas with shortage of healthcare professionals, extends the traditional RBAC [10] model, while retaining its advantages (such as ability to define and manage complex security policies). The model dynamically adjusts Location Assignment and Permission Assignment based on location, and other contextual, information gathered.

The rest of this paper is organised as follows. Section 2 presents an overview of the background work where various access control models are discussed. Section 3 presents the dynamic Role-And-Context Based Access Control model, which is an extension of the traditional Role-Based Access Control model. Section 4 presents the conclusion and future work.

Background

In computing, access control refers to security features that control which principals (can be *persons, processes and machines*) have access to which resources.

Several access control models [10-13] have been developed to ensure the security of sensitive information. Among the common models include Mandatory Access Control (MAC), Discretionary Access Control (DAC)

Role-Based Access Control (RBAC), Team-Based Access Control (TMAC), and Attribute-Based Access Control (ABAC).

From these and other models, RBAC, which associates users to roles and roles to permissions, has proved to be more popular and is considered as an efficient way of assigning access rights to users while at the same time ensuring data security [12]. Despite its popularity, RBAC is criticised for its difficulty in setting up an initial role structure and for its inflexibility in rapidly changing environments like healthcare [12]. Additionally for the areas with the shortage of healthcare professionals, in this paper we argue that, the usage of traditional RBAC, in the healthcare domain, might result in lack of services to patients. To cater for such environments, RBAC needs to be extended with dynamic contextual attributes, and for this paper location information is mainly proposed. Section 3 presents the dynamic Role-And-Context Based Access Control model.

RAC-BAC Model

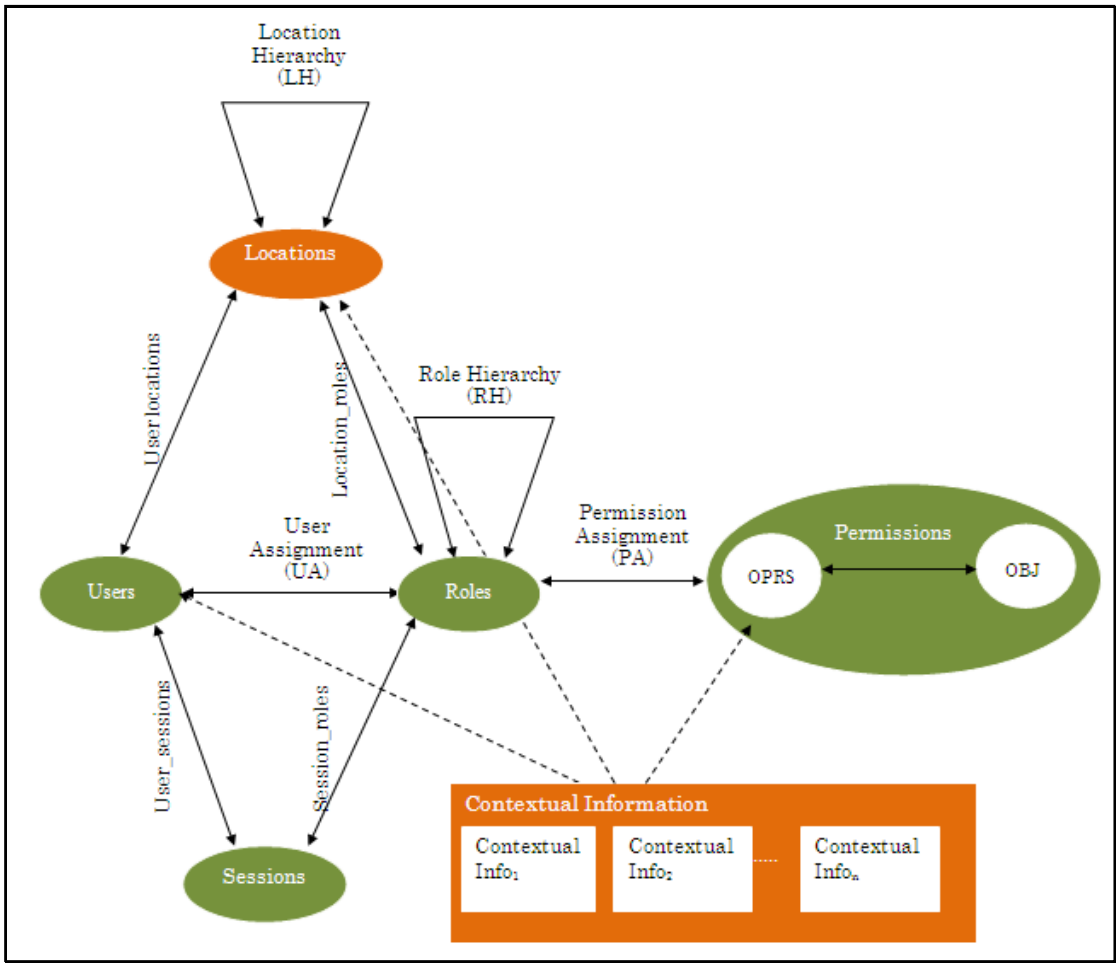
As highlighted in related work section, the approach adopted for this work involves re-modelling and extending the traditional RBAC model with contextual information, and to be more precise this work is much more focused on modelling location information.

The extended model from the traditional RBAC model, as presented in figure 1, introduces the notion of Location Assignment (LA), which is a relation between Location and Role. The model dynamically adjusts Location Assignments and Permission Assignments based on contextual information gathered. In our approach, each user of the system is assigned a temporary role depending on location, and other information, from where access to records is made.

Rather than only addressing access control requirements for the general healthcare environment [8], the presented model, which can be used in various applications, is considered appropriate for controlling access to sensitive records in areas where there is a limited number of professionals.

Additionally, as traditional RBAC lacks the ability to support expression of access control that refer to the condition of the system [14, 15] then with this model, the idea is to use both dynamic (such as, user’s location), and static (such as, user ID) contextual information for authorisation constraints while making access control decisions.

Figure 1



Proposed Access Control Model

Conclusion and Future Work

Although access control is a well known and used concept in various domains, its usage for the areas with the limited number of professionals is considered minimal. In this paper we have presented an approach for extending the usage of location information, in the healthcare domain, to improve the security of patient's records for the areas with the shortage of healthcare professionals. As for future work, the presented model will be formally defined and a prototype system will be developed before its evaluation.

References

[1] J. Krumm, "A survey of computational location privacy," *Personal and Ubiquitous Computing*, vol. 13, pp. 391-399, 2009.

[2] M. Skubic, G. Alexander, M. Popescu, M. Rantz, and J. Keller, "A smart home application to eldercare: Current status and lessons learned," *Technology and Health Care*, vol. 17, pp. 183-201, 2009.

[3] Z. Lv, F. Xia, G. Wu, L. Yao, and Z. Chen, "iCare: A Mobile Health Monitoring System for the Elderly," in *Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications \& Int'l Conference on Cyber, Physical and Social Computing*, 2010, pp. 699-705.

[4] Z. Omary, F. Mtenzi, B. Wu, and C. O'Driscoll, "Accessing sensitive patient information in ubiquitous healthcare systems," in *International Conference for Internet Technology and Secured Transactions (ICITST)*, London 2010, pp. 1-3.

[5] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati, "Supporting location-based conditions in access control policies," 2006, pp. 212-222.

[6] H. Schulzrinne and R. Marshall, "Requirements for emergency context resolution with internet technologies," RFC 5012, January 2008.

[7] Z. Omary, F. Mtenzi, and B. Wu, "Context for Securing EHRs in a Dynamic Healthcare Environment," in *The 5th International Conference on Information Technology*, Amman, Jordan, 2011.

[8] K. Beznosov, "Requirements for access control: US healthcare domain," 1998.

[9] H. B. Funk and C. A. Miller, "Location Modeling for Ubiquitous Computing: Is This Any Better?," *LOCATION MODELING FOR UBIQUITOUS COMPUTING*, p. 29, 2001.

[10] R. S. Sandhu, "Role-based access control," *Advances in computers*, vol. 46, pp. 237-286, 1998.

[11] J. B. Deng and F. Hong, "Task-Based access control model," *Journal of Software*, vol. 14, pp. 76-82, 2003.

[12] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," *Computer*, vol. 43, pp. 79-81.

[13] R. K. Thomas, "Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments," in *Proceedings of the second ACM workshop on Role-based access control*, Fairfax, Virginia, United States, 1997, pp. 13-19.

[14] R. Araujo and S. Gupta, "Design authorisation systems using SecureUML," *Foundstone Professional Services*, pp. 2-16, 2005.

[15] L. Gomez, L. Moraru, D. Simplot-Ryl, and K. Wrona, "Using sensor and location information for context-aware access control," in *EUROCON2005*, Serbia and Montenegro, 2005, pp. 68-71